

SUPREME COURT OF CANADA

CITATION: R. v. Morelli, 2010 SCC 8

DATE: 20100319 **DOCKET:** 32741

BETWEEN:

Urbain P. Morelli Appellant and Her Majesty The Queen Respondent

CORAM: McLachlin C.J. and Binnie, Deschamps, Fish, Abella, Charron and Rothstein JJ.

REASONS FOR JUDGMENT: (paras. 1 to 113)

Fish J. (McLachlin C.J. and Binnie and Abella JJ. concurring)

DISSENTING REASONS: (paras. 114 to 183)

Deschamps J. (Charron and Rothstein JJ. concurring)

NOTE: This document is subject to editorial revision before its reproduction in final form in the *Canada Supreme Court Reports*.

R. v. MORELLI

Urbain P. Morelli

Appellant

ν.

Her Majesty The Queen

Respondent

Indexed as: R. v. Morelli

Neutral citation: 2010 SCC 8.

File No.: 32741.

2009: February 18; 2010: March 19.

Present: McLachlin C.J. and Binnie, Deschamps, Fish, Abella, Charron and Rothstein JJ.

ON APPEAL FROM THE COURT OF APPEAL FOR SASKATCHEWAN

Constitutional law — Charter of Rights — Search and seizure — Validity of search warrant — Police obtaining warrant to search accused's computer — Pornographic pictures involving children found and accused convicted of possession of child pornography — Whether search warrant issued on basis of misleading, inaccurate and incomplete information — Whether search of computer breached accused's rights under s. 8 of Canadian Charter of Rights and Freedoms — If so, whether evidence ought to be excluded pursuant to s. 24(2) of Charter.

Criminal law — Search warrant — Validity — Police obtaining warrant to search accused's computer — Pornographic pictures involving children found and accused convicted of possession of child pornography — Whether there were reasonable grounds to issue search warrant — Whether search warrant issued on basis of misleading, inaccurate and incomplete information.

Criminal law — Possession of child pornography — Elements of offence — Definition of possession — Whether possession of illegal image in computer means possession of underlying data file — Whether possession can be established even if accused did not download image — Criminal Code, R.S.C. 1985, c. C-46, ss. 4(3), 163.1(4).

On September 5, 2002, a computer technician arrived unannounced at the accused's house to install a high-speed Internet connection the accused had ordered. The accused lived with his wife and two children, aged three and seven, but was alone that day with his younger daughter. When the technician opened the accused's Web browser, he noticed several links to both adult and child pornography sites in the taskbar's "favourites" list, including two that were labelled "Lolita Porn" and "Lolita XXX". He also saw a legal pornographic image, but he could not remember afterwards if it was on the browser's home page or on the computer desktop. In the room, he noticed home videos and, on a tripod, a webcam that was connected to a videotape recorder and was pointed at the toys and at the child. Unable to finish his work on that day, the technician returned the

following morning and noted that everything had been "cleaned up": the child's toys had been placed in a box, the videotapes could no longer be seen, the webcam was pointed at the computer user's chair and the computer hard drive had been "formatted". In November, concerned with the child's safety, the technician reported what he had seen to a social worker, who contacted the RCMP. The technician made a statement to Cst. O in January 8, 2003. After the interview, O consulted Cpl. B from the RCMP's Technological Crime Unit, who he knew had experience investigating crimes involving computers and technological devices. B stated that these types of offenders were habitual and would continue their computer practices with child pornography and that this information would remain inside the hard drive of the computer. O also spoke to Cst. H who, he had been told by a Crown attorney, had experience investigating child exploitation offences. Hinformed O that these offenders treasured collections on their computers and liked to store them and create backups. O also verified whether an active Internet connection was still being provided to the accused's residence. He then drafted an information to obtain a search warrant ("ITO") and, on January 10, a warrant was issued pursuant to s. 487 of the Criminal Code to search the accused's computer. Pornographic pictures involving children were found on the computer and the accused was charged with possession of child pornography contrary to s. 163.1(4) of the Criminal Code. At trial, he unsuccessfully challenged the validity of the search warrant under s. 8 of the Canadian Charter of Rights and Freedoms. The trial judge convicted the accused and the majority of the Court of Appeal upheld the conviction.

Held (Deschamps, Charron and Rothstein JJ. dissenting): The appeal should be allowed. The accused's conviction is quashed and an acquittal is entered.

Per McLachlin C.J. and Binnie, Abella and Fish JJ.: The ITO is limited to allegations of possession of child pornography contrary to s. 163.1(4) of the Criminal Code and does not involve allegations of accessing child pornography pursuant to s. 163.1(4.1). Merely viewing in a web browser an illegal image stored in a remote location on the Internet does not establish the level of control necessary to find possession. Neither does creating a "favourite" or an "icon" on one's computer. In order to commit the offence of possession, as opposed to the offence of accessing of child pornography, one must knowingly acquire the underlying data files and store them in a place under one's control. It is the underlying data file that is the stable "object" that can be transferred, stored, and possessed. The automatic caching of a file to the hard drive does not, without more, constitute possession. While the cached file might be in a "place" over which the computer user has control, in order to establish possession it must be shown that the file was knowingly stored and retained through the cache. An ITO seeking a warrant to search for evidence of possession, rather than accessing, must therefore provide reasonable grounds to believe that the alleged offender possesses (or has possessed) digital files of an illegal image, and that evidence of that possession will be found in the place to be searched at the time the warrant is sought. Here, the search and seizure of the accused's computer infringed his right under s. 8 of the Charter. Even when corrected and amplified on review, the ITO was insufficient to permit any justice of the peace, acting reasonably, to find adequate grounds for the search. The ITO did not allege the distinct and separate offence of accessing child pornography and, stripped of its defects and deficiencies, all that really remained were two Internet links, seen four months earlier in the "Favourites" menu of a web browser on a computer that was subsequently formatted, deleting both links. The prior presence of the two "Lolita" links supports a reasonable inference that the accused browsed a website that contained explicit images of females under the age of 18, but this does not suffice to establish possession.

The misleading passages in the ITO that suggested that the technician had actually viewed illegal pornography on the computer, rather than suspiciously labelled "favourites", must be excised. That pornographic images of children were actually seen on the computer is an entirely false claim. Aside from false statements, the ITO in several places gave an incomplete and misleading account of the facts, in contravention of the informant's duty to make full and frank disclosure of all material information. The ITO does not mention, as the *voir dire* revealed, that the two "favorites" were "just scattered through the favourites" among additional links pointing to "regular adult material". The failure to mention these facts creates a misleading impression. Once it is understood that the suspicious "Favourites" were in fact exceptions, found together with much more material that was undisputedly legal, the inference that the accused possessed illegal images becomes significantly less compelling. Furthermore, the descriptions of the webcam and its placement are juxtaposed immediately alongside the descriptions of the suspicious "Favourites" and the technician's claims that he had "observed 'Lolita Porn'", clearly suggesting that the accused might have been making (and possessing) his own illegal pornography. The ITO, however, did not include a number of additional facts known to the police. First, the three-year- old child mentioned, but not identified, in the ITO was in fact the accused's daughter. Second, the ITO stated that the accused was alone in the house with the girl, but failed to mention that his wife lived with them. Third, the ITO also failed to mention that the child was fully clothed, that there was no evidence of abuse, that the computer room had a child gate and appeared to double as a playroom for the child, and that the child was playing with the scattered toys in the middle of the room when the technician arrived. While the reviewing judge found no deliberate attempt to mislead, it is nonetheless evident that the police officer's selective presentation of the facts painted a less objective and more villainous picture

than the picture that would have emerged had he disclosed all the material information available to him at the time. It seems much more plausible that the accused was simply using the VCR and webcam to videotape his young daughter at play for posterity's sake, rather than for any purpose connected to child pornography.

To conclude that evidence of possession would be found four months after the hard drive was erased, one must accept either that the accused had made external copies of illegal images present in the computer before formatting its hard drive or that he acquired additional illegal images after the formatting. While the ITO seeks to establish inferences based on the likely behaviour of the accused on the basis of generalizations made by B and H about the propensities of certain "types of offenders" to hoard and copy illegal images, the ITO does not establish either the veracity of the generalization about the alleged "type of offender", or that the accused is in fact the "type" to which the generalization might have applied. The ITO contains no evidentiary material in this regard apart from the bald assertion of the two police officers and there is virtually nothing to describe, let alone establish, the expertise of the officers. Moreover, the class of persons to whom specific proclivities are attributed is defined so loosely as to bear no real significance. There is no reason to believe, on the basis of the information in the ITO as amplified, that all child pornography offenders engage in hoarding, storing, sorting, and categorizing activity. To permit reliance on broad generalizations about loosely defined classes of people is to invite dependence on stereotypes and prejudices in lieu of evidence. It is not the role of courts to establish by judicial fiat broad generalizations regarding the "proclivities" of certain "types" of people, including offenders. Matters of this sort are best left to be established by the Crown, according to the relevant standard — in this case, reasonable grounds for belief. Here, two suspiciously labelled links in the "Favourites" do not suffice to characterize a

person as an habitual child pornography offender of the type that seeks out and hoards illegal images. The fact that the bulk of the pornographic material that the technician observed at the accused's house was legal adult pornography suggests that the accused did not have a "pronounced" interest in child pornography.

The presence of the webcam, which was functioning as a camcorder recording to a VCR, has only a tenuous relation to the crime alleged. While it may be true that the accused was adept at recording videotapes and storing the tapes for future use — as is nearly everyone who owns a camcorder — this says nothing about his propensity to store a different kind of image (child pornography), in a different medium (a computer, as opposed to videotape), acquired in a different manner (downloading, as opposed to filming). To draw an inference that he is of the type to hoard illegal images is to speculate impermissibly. Nor does the accused's conduct after the technician's visit support the conclusion that he was the sort of person to seek out and hoard child pornography. The accused might well have tidied up the room and formatted his computer simply to avoid further embarrassment from having an outsider see the disorderly state of his home and the evidence of his consumption of pornography on his computer. The accused's conduct might raise suspicions but, as a matter of law, mere suspicion is no substitute for reasonable grounds.

The evidence obtained as a result of the illegal search should be excluded under s. 24(2) of the *Charter*. When the three relevant factors are balanced, admitting the illegally obtained evidence in this case would bring the administration of justice into disrepute. The trial judge found no deliberate attempt to mislead and no deliberate misconduct on the part of the officer who swore the ITO, but the repute of the administration of justice would nonetheless be significantly eroded,

particularly in the long term, if criminal trials were permitted to proceed on the strength of evidence obtained from the most private "place" in the home on the basis of misleading, inaccurate, and incomplete ITOs upon which a search warrant was issued. The public must have confidence that invasions of privacy are justified, in advance, by a genuine showing of probable cause.

Per **Deschamps**, Charron and Rothstein JJ. (dissenting): A specific intention to deal with the object in a particular manner is not an element of the offence of possession of child pornography. Sections 4(3) and 163.1(4) of the *Criminal Code* indicate that possession of child pornography is criminal in and of itself, irrespective of the use to which the accused intends to put the prohibited material. The requisite *mens rea* will be established at trial if it is shown that the accused willingly took or maintained control of the object with full knowledge of its character. The accused does not need to have control in a place belonging to him or her, such as his or her hard drive. The provision simply requires the material to be "in any place" for the use or benefit of the accused. Therefore, even if an accused does not actually download offending material, possession is established if the accused has control over the material for his or her use or benefit or for that of someone else. When applying for a search warrant, it is sufficient that there be credible evidence to support a reasonable belief that the search will provide evidence of commission of the offence.

Although the ITO could have been more elaborate in many respects, the omissions the accused complains of do not support a conclusion that the ITO was so deficient that it did not provide the authorizing judge with a sufficiently credible factual basis. The information concerning the presence of the child, the toys, and the webcam was necessary to convey to the authorizing judge the technician's concerns about the safety of the child. From this perspective, the facts that the

accused was the child's father and that he resided with his wife, which were not mentioned in the ITO, were not determinative since, in the technician's mind, what was at stake was the safety of a child. The references in the ITO to the removal of child pornography from the accused's computer cannot be characterized as false. Viewed in context, there is no question that what had, according to the technician, been removed from the computer were the links in the "favourites" list to child pornography. Therefore the authorizing judge must have understood this to be the case. Since there is no indication that the allegations or references were meant to mislead or were so lacking in informational context, they should not be expunged from the ITO.

It was neither inappropriate nor erroneous to rely on the information provided by officers B and H about the propensity of child pornography offenders to collect and hoard such materials. This propensity, which seems to be notorious, has been accepted in numerous child pornography cases as part of the factual backdrop giving rise to reasonable grounds for issuing search warrants. While more contextual information on both the subject matter and the source would have made it easier to understand and assess the officers' statements, there is no indication that they were not qualified or that there was any intention to mislead. Consequently, it was open to the reviewing judge to receive evidence which amplified the information and conclude that the authorizing judge was provided with sufficient evidence. The positions the officers held in their respective forces were also enough to support a conclusion that their statements had sufficient probative value to be included in the ITO. Lastly, the officers did not state that the accused was a habitual child pornography offender. The conversations between O and the other officers took place several months after the technician's visits, and they related to what material might be found in the computer and whether material would still be found there despite the time elapsed between the visits and the

swearing of the ITO. These are facts that O had to put before the authorizing judge.

Although there was a four-month delay between the technician's visits and the swearing of the ITO, it was reasonable for the authorizing judge to conclude that the accused still had the computer in question in his residence and that any "child pornography" was still in the house. There was adequate information in the ITO about the storage of the materials, and no reason to presume that the accused would have changed his computer after the visits and no indication that the computer was in any way in need of being replaced. It was therefore appropriate for O to rely on common sense and on the ongoing subscription to an Internet connection to support his allegation that the computer was still in the accused's residence. The police officers' statements concerning the proclivity of child pornography users to save and collect such material could also serve as a basis for concluding that it was reasonable to believe that, if the accused was this type of offender, evidence of the offence would still be found in the computer after four months.

In this case, the facts alleged in the ITO, as amplified at the *voir dire*, were sufficient for the reviewing judge to conclude that there was a basis for the authorizing judge's decision to issue the warrant. The facts that there were several links to both adult and child pornography in the "favourites" list and that a "graphic" pornographic image was prominently displayed on the computer justified the authorizing judge's drawing the reasonable inference that the accused had a conspicuous interest in this type of material. The position of the camera and the fact that it was connected to a videotape recorder at the time of the technician's first visit, together with the presence of both labelled and unlabelled videotapes, showed that he was interested in reproducing images, accumulating such material, and keeping it for his future use. The accused's desire not to arouse suspicion with respect to his reproduction of images or his computer practices could reasonably be inferred from his actions after being informed that the technician needed to return. There was a credibly based probability that the accused was in the habit of reproducing and saving images and had a propensity to pornography, and more specifically to child pornography. While the police officers' statements could not be used to demonstrate that he was a type of person who was likely to be in possession of child pornography, given that there is credible independent evidence of this, they do shed light on the implications of that evidence. In these circumstances, the statements that child pornography offenders are collectors could only make it more likely that evidence of the possession of prohibited material would still exist at the time the ITO was drafted.

Cases Cited

By Fish J.

Applied: *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; referred to: Beaver v. The Queen, [1957] S.C.R. 531; *R. v. Panko* (2007), 52 C.R. (6th) 378; *R. v. Weir*, 2001 ABCA 181, 95 Alta. L.R. (3d) 225; *R. v. Daniels*, 2004 NLCA 73, 242 Nfld. & P.E.I.R. 290; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992; *R. v. Fawthrop* (2002), 161 O.A.C. 350; *United States v. Weber*, 923 F.2d 1338 (1990); *United States v. Terry*, 522 F.3d 645 (2008); *R. v. Graham*, 2008 PESCAD 7, 277 Nfld & P.E.I.R. 103.

By Deschamps J. (dissenting)

R. v. Debot, [1989] 2 S.C.R. 1140; Baron v. Canada, [1993] 1 S.C.R. 416; Hunter v. Southam Inc., [1984] 2 S.C.R. 145; Illinois v. Gates, 462 U.S. 213 (1983); R. v. Garofoli, [1990] 2 S.C.R. 1421; R. v. Grant, [1993] 3 S.C.R. 223; R. v. Araujo, 2000 SCC 65, [2000] 2 S.C.R. 992; Quebec (Attorney General) v. Laroche, 2002 SCC 72, [2002] 3 S.C.R. 708; R. v. Pires, 2005 SCC 66, [2005] 3 S.C.R. 343; R. v. York, 2005 BCCA 74, 193 C.C.C.(3d) 331; R. v. Chalk, 2007 ONCA 815, 88 O.R. (3d) 448; R. v. Terrence, [1983] 1 S.C.R. 357; R. v. Hess (No. 1) (1948), 94 C.C.C. 48; Beaver v. The Queen, [1957] S.C.R. 531; R. v. Weir, 2001 ABCA 181, 95 Alta. L.R. (3d) 225; R. v. Daniels, 2004 NLCA 73, 242 Nfld. & P.E.I.R. 290; R. v. Neveu, 2005 NSPC 51, 239 N.S.R. (2d) 59; R. v. Fawthrop (2002), 161 O.A.C. 350; United States v. Gourde, 440 F.3d 1065 (2006); United States v. Martin, 426 F.3d 68 (2005); United States v. Shields, 458 F.3d 269 (2006); Davidson v. United States, 213 Fed.Appx. 769 (2006); United States v. Falso, 544 F.3d 110 (2008); United States v. Perrine, 518 F.3d 1196 (2008); R. v. Mohan, [1994] 2 S.C.R. 9; R. v. J.-L.J., 2000 SCC 51, [2000] 2 S.C.R. 600; R. v. Trochym, 2007 SCC 6, [2007] 1 S.C.R. 239; R. v. Graham, 2007 CarswellPEI 80, aff'd 2008 PESCAD 7, 277 Nfld & P.E.I.R. 103; United States v. Terry, 522 F.3d 645 (2008); R. v. Arcuri, 2001 SCC 54, [2001] 2 S.C.R. 828.

Statutes and Regulations Cited

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

Criminal Code, R.S.C. 1985, c. C-46, ss. 4(3), 163.1(4), (4.1), (4.2), (6), 487.

Authors Cited

- Akdeniz, Yaman. Internet Child Pornography and the Law: National and International Responses. Burlington, Vermont: Ashgate, 2008.
- Canada. House of Commons. *House of Commons Debates*, vol. 137, 1st Sess., 37th Parl., May 3, 2001, p. 3581.
- Howard, Ty E. "Don't Cache Out your Case: Prosecuting Child Pornography Posssession Law Based on Images Located in Temporary Internet Files" (2004), 19 *Berkeley Tech. L.J.* 1227.
- Luehr, Paul H. "Real Evidence, Virtual Crimes: The Role of Computer Forensic Experts" (2005-2006), 20 Crim. Just. 14.
- Marin, Giannina. "Possession of Child Pornography: Should You Be Convicted When the Computer Cache Does the Saving for You?" (2008), 60 *Fla. L. Rev.* 1205.
- Michaels, Rebecca, "Criminal Law The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should Be Criminal" (2008), 30 W. New Eng. L. Rev. 817.
- Taylor, Max, and Ethel Quayle. Child Pornography: An Internet Crime. London: Routledge,

2003.

APPEAL from a judgment of the Saskatchewan Court of Appeal (Jackson, Richards and

Hunter JJ.A.), 2008 SKCA 62, 310 Sask. R. 165, 423 W.A.C. 165, 233 C.C.C. (3d) 465, 172 C.R.R.

(2d) 167, [2008] 7 W.W.R. 191, [2008] S.J. No. 300 (QL), 2008 CarswellSask 300, upholding the

accused's conviction. Appeal allowed, Deschamps, Charron and Rothstein JJ. dissenting.

Aaron A. Fox, Q.C., and Jeffrey Beedell, for the appellant.

Anthony B. Gerein, for the respondent.

The judgment of McLachlin C.J. and Binnie, Fish and Abella JJ. was delivered by

FISH J. —

Ι

[1] This case concerns the right of everyone in Canada, including the appellant, to be secure against unreasonable search and seizure. And it relates, more particularly, to the search and seizure of personal computers.

[2] It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.

[3] First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident. [4] That is precisely the kind of search that was authorized in this case. And it was authorized on the strength of an Information to Obtain a Search Warrant ("ITO") that was carelessly drafted, materially misleading, and factually incomplete. The ITO invoked an unsupported stereotype of an ill-defined "type of offender" and imputed that stereotype to the appellant. In addition, it presented a distorted portrait of the appellant and of his surroundings and conduct in his own home at the relevant time.

[5] Even when corrected and amplified on review, the ITO was insufficient to permit any justice of the peace, acting reasonably, to find adequate grounds for the search. Stripped of its defects and deficiencies, all that really remained were two Internet links, seen four months earlier in the "Favourites" menu of a Web browser — on a computer that was subsequently formatted, *deleting both links*.

[6] The ITO alleged that the appellant was then in possession of child pornography and that there were reasonable and probable grounds to believe that "the said material, or some part of them [*sic*] are contained inside the computer". I emphasize from the outset that the ITO did not allege the distinct and separate offence of *accessing* child pornography, either when the ITO was sworn or four months earlier, before the computer was formatted.

[7] As we shall see, the essential elements of the alleged offence, the time of its alleged commission, and the complete lack of evidence that there was child pornography in the computer when the ITO was sworn all underscore the manifest inadequacy of the ITO and the

unreasonableness of the search that ensued.

[8] To be sure, offences involving child pornography are particularly insidious. They breed a demand for images that exploit vulnerable children, both economically and morally. Understandably, offences of this sort evoke a strong emotional response. They generate widespread condemnation and intense feelings of disapprobation, if not revulsion.

[9] It is for this very reason that the police, in enforcing the law, must avoid any temptation to resort to stereotypical, inflammatory, or misleading allegations. And where they yield to that temptation, courts must be particularly vigilant to issue process, or subsequently validate the issuance of process, only where reasonable and probable grounds for a search or an arrest are in fact made out. While the law must be relentlessly enforced, legal requirements must be respected, and constitutional safeguards preserved.

[10] Unlike Justice Deschamps and with the greatest of respect, I am satisfied that the record discloses no reasonable and probable grounds for the search and seizure of the appellant's computer. I agree with Richards J.A., dissenting in the Court of Appeal, that the search and seizure therefore infringed the appellant's constitutional right, under s. 8 of the *Canadian Charter of Rights and Freedoms*, "to be secure against unreasonable search or seizure".

[11] Applying the test recently set out in *R. v. Grant*, 2009 SCC 32 [2009] 2 S.C.R. 353, I believe we are bound, in virtue of s. 24(2) of the *Charter*, to exclude the evidence thus obtained. In the absence of this illegally obtained evidence, the appellant could not reasonably have been convicted. Accordingly, like Justice Richards, I would allow the appeal, set aside the appellant's

conviction, and enter an acquittal in its place.

Π

[12] The search warrant in this case was issued on the strength of an Information alleging that the appellant was then in possession of child pornography, contrary to s. 163.1(4) of the *Criminal Code*, R.S.C. 1985, c. C-46. The Information alleged as well that the pornographic materials in question were "contained inside" the appellant's personal computer.

[13] The threshold question on this appeal is whether the justice of the peace who issued the search warrant acted on reasonable and probable grounds, as required under both the *Criminal Code* and the *Charter*. To answer that question, it is necessary to first understand when one may properly be said to "possess" an image in a computer, within the meaning of s. 163.1 of the *Criminal Code*.

[14] In my view, merely viewing in a Web browser an image stored in a remote location on the Internet does not establish the level of control necessary to find possession. Possession of illegal images requires *possession of the underlying data files in some way*. Simply viewing images online constitutes the separate crime of *accessing* child pornography, created by Parliament in s. 163.1(4.1) of the *Criminal Code*.

[15] For the purposes of the *Criminal Code*, "possession" is defined in s. 4(3) to include *personal possession, constructive possession*, and *joint possession*. Of these three forms of culpable possession, only the first two are relevant here. It is undisputed that *knowledge* and *control* are

essential elements common to both.

[16] On an allegation of *personal possession*, the requirement of knowledge comprises two elements: the accused must be aware that he or she has physical custody of the thing in question, and must be aware as well of what that thing is. Both elements must co-exist with an act of control (outside of public duty): *Beaver v. The Queen*, [1957] S.C.R. 531, at pp. 541-42.

[17] *Constructive* possession is established where the accused did not have physical custody of the object in question, but did have it "in the actual possession or custody of another person" or "in any place, whether or not that place belongs to or is occupied by him, for the use or benefit of himself or of another person." (*Criminal Code*, s. 4(3)(a)). Constructive possession is thus complete where the accused: (1) has knowledge of the character of the object, (2) knowingly puts or keeps the object in a particular place, whether or not that place belongs to him, and (3) intends to have the object in the particular place for his "use or benefit" or that of another person.

[18] Here, the appellant is alleged to have had possession of digital images in a computer, rather than tangible objects. The law of possession, however, developed in relation to physical, concrete objects. Its extension to virtual objects — in this case, images stored as digital files and displayed on computer monitors — presents conceptual problems. Unlike traditional photographs, the digital information encoding the image — the image file — can be possessed even if no representation of the image is visible. Likewise, even if displayed on a person's computer monitor, the underlying information might remain firmly outside that person's possession, located on a server thousands of kilometres away, over which that person has no control.

[19] Essentially, there are thus two potential "objects" of possession of an image in a computer — the image file and its decoded visual representation on-screen. The question is whether one can ever be said to be in culpable possession of the visual depiction alone, or whether one can only culpably possess the underlying file. Canadian cases appear implicitly to accept only the latter proposition: That possession of an image in a computer means *possession of the underlying data file*, not its mere visual depiction.

[20] Three Canadian appellate decisions illustrate the point.

[21] In *R. v. Panko* (2007), 52 C.R. (6th) 378, the Ontario Superior Court of Justice held that possession might be established on the basis of icons on the desktop that pointed to illegal images *stored* on the computer's own hard drive.

[22] In *R. v. Weir*, 2001 ABCA 181, 95 Alta. L.R. (3d) 225, the Alberta Court of Appeal confirmed the validity of a search warrant obtained on information that prohibited images were attached to an e-mail message received by the accused but not yet opened. The court rejected the submission that the search warrant had been issued for an anticipated offence because it was a reasonable inference that the files would have already been *downloaded* onto the accused's computer at the time the warrant was authorized.

[23] Finally, in *R. v. Daniels*, 2004 NLCA 73, 242 Nfld & P.E.I.R. 290, the Newfoundland and Labrador Court of Appeal found that possession began at the moment the accused began

downloading the illegal image files to his hard drive, even though the download was interrupted and the images were never viewed.

[24] In all three cases, the courts proceeded on the understanding that the object illegally possessed by the accused was the image *file*, not a visual display or rendering of the image.

[25] This is a sensible interpretation for a number of reasons. First, and most important, because Parliament, in s. 163.1(4.1) of the *Criminal Code*, has made accessing illegal child pornography a separate crime, different from possession. In virtue of s. 163.1(4.2), a person accesses child pornography by "knowingly caus[ing the] child pornography to be viewed by, or transmitted to, himself or herself".

[26] Parliament's purpose in creating the offence of accessing child pornography, as explained by the then Minister of Justice, was to "capture those who intentionally view child pornography on the [Inter]net but where the legal notion of possession may be problematic" (Hon. Anne McLellan, *House of Commons Debates*, vol. 137, 1st Sess., 37th Parl., May 3, 2001, at p. 3581).

[27] What made a charge of possession "problematic", of course, is that possessing a digital file and viewing it are discrete operations — one could be criminalized without also criminalizing the other. In the case of child pornography, Parliament has now criminalized both. But viewing and possession should nevertheless be kept conceptually separate, lest the criminal law be left without the analytical tools necessary to distinguish between storing the underlying data file and merely

viewing the representation that is produced when that data, residing elsewhere, is decoded. The ITO here is specifically limited to allegations of possession pursuant to s. 163.1(4) of the *Criminal Code* (ITO, preamble and paras. 2, 4 and 16).

[28] Interpreting possession to apply only to the underlying data file is also more faithful to a traditional understanding of what it means to "possess" something. The traditional objects of criminal possession — for example, contraband, drugs, and illegal weapons — are all things that could, potentially at least, be transferred to another person.

[29] Without storing the underlying data, however, an image on a screen cannot be transferred. The mere possibility of sharing a *link* to a Website or enlarging the visual depiction of a Website, as one could "zoom in" on a TV screen image, is insufficient to constitute control over the content of that site. It is indeed the underlying data file that is the stable "object" that can be transferred, stored, and, indeed, possessed. More broadly, the object possessed must itself have some sort of permanence.

[30] Thus, while it does not matter for the purposes of criminal possession how briefly one is in possession of the object, the thing said to be culpably possessed cannot — like a broadcast image flickering across a TV screen or a digital image displayed transiently on-screen — be essentially evanescent.

[31] Plainly, the mere fact that an image has been accessed by or displayed in a Web browser does not, without more, constitute possession of that image. An ITO seeking a warrant to search for

evidence of possession (rather than accessing) must therefore provide reasonable and probable grounds to believe that the alleged offender possesses (or has possessed) digital files of an illegal image, and that evidence of that possession will be found in the place to be searched. It is not enough to provide reasonable and probable grounds to believe that the alleged offender viewed or accessed illegal images using a computer, without knowingly taking possession — which includes control — of the underlying files in some way.

[32] In applying these principles to the facts of this case, I take care not to be understood to have circumscribed or defined constructive possession of virtual objects. I leave open the possibility, for example, that one could constructively possess a digital file without downloading it to his or her hard drive, using for example a Web-based e-mail account to store illegal material.

[33] In short, my purpose here is not to say what constructive possession of virtual objects *necessarily is*, but rather what it *manifestly is not*. Plainly, in my view, previous access and the possibility of again accessing a Website that contains digital images, located on a distant server over which the viewer has no control, do not constitute — either alone or together — constructive possession. However elastic the notion of constructive possession may be, to stretch it that far is to defy the limits of its elasticity.

[34] For the sake of greater clarity, I turn now to consider how this understanding of possession applies to files in an Internet cache (that is, copies of files automatically stored on the hard drive by a Web browser).

[35] When accessing Web pages, most Internet browsers will store on the computer's own hard drive a temporary copy of all or most of the files that comprise the Web page. This is typically known as a "caching function" and the location of the temporary, automatic copies is known as the "cache". While the configuration of the caching function varies and can be modified by the user, cached files typically include images and are generally discarded automatically after a certain number of days, or after the cache grows to a certain size.

[36] On my view of possession, the automatic caching of a file to the hard drive does not, without more, constitute possession. While the cached file might be in a "place" over which the computer user has control, in order to establish possession, it is necessary to satisfy *mens rea* or fault requirements as well. Thus, it must be shown that the file was *knowingly* stored and retained through the cache.

[37] In the present case, the charge is not based on the appellant using his cache to possess child pornography. It is hardly surprising as most computer users are unaware of the contents of their cache, how it operates, or even its existence. Absent that awareness, they lack the mental or fault element essential to a finding that they culpably possess the images in their cache. Having said that, there may be rare cases where the cache is *knowingly* used as a location to store copies of image files with the *intent* to retain possession of them through the cache.

[38] Justice Deschamps has advanced a more expansive conception of possession, under which simply viewing an image might, in some circumstances at least, constitute possession. As I will presently explain, even if one were to adopt my colleague's view, the ITO in this case fails to establish reasonable and probable grounds for the impugned search of the appellant's computer.

III

[39] Under the *Charter*, before a search can be conducted, the police must provide "reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search" (*Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 168). These distinct and cumulative requirements together form part of the "minimum standard consistent with s. 8 of the *Charter* for authorizing search and seizure" (p. 168.)

[40] In reviewing the sufficiency of a warrant application, however, "the test is whether there was reliable *evidence that might reasonably be believed on the basis of which the authorization could have issued*" (*R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 54 (emphasis in original)). The question is not whether the reviewing court would itself have issued the warrant, but whether there was sufficient credible and reliable evidence to permit a justice of the peace to find reasonable and probable grounds to believe that an offence had been committed and that evidence of that offence would be found at the specified time and place.

[41] The reviewing court does not undertake its review solely on the basis of the ITO as it was presented to the justice of the peace. Rather, "the reviewing court must exclude erroneous information" included in the original ITO (*Araujo*, at para. 58). Furthermore, the reviewing court may have reference to "amplification" evidence — that is, additional evidence presented at the *voir*

dire to correct minor errors in the ITO — so long as this additional evidence corrects good faith errors of the police in preparing the ITO, rather than deliberate attempts to mislead the authorizing justice.

[42] It is important to reiterate the limited scope of amplification evidence, a point well articulated by Justice LeBel in *Araujo*. Amplification evidence is not a means for the police to adduce additional information so as to retroactively authorize a search that was not initially supported by reasonable and probable grounds. The use of amplification evidence cannot in this way be used as "a means of circumventing a prior authorization requirement" (*Araujo*, at para. 59).

[43] Rather, reviewing courts should resort to amplification evidence of the record before the issuing justice only to correct "some minor, technical error in the drafting of their affidavit material" so as not to "put form above substance in situations where the police had the requisite reasonable and probable grounds and had demonstrated investigative necessity but had, in good faith made" such errors (para 59). In all cases, the focus is on "the information available to the police at the time of the application" rather than information that the police acquired after the original application was made (para. 59).

IV

[44] The deficiencies of the ITO in this case must be addressed in some detail before determining whether it could support the issuance of the warrant. In particular, there are erroneous statements that must be excised, and there are numerous omissions that violate "[t]he legal obligation

on anyone seeking an *ex parte* authorization [to make] *full and frank* disclosure of *material facts*" (*Araujo*, at para. 46 (emphasis in original)). Once these flaws are taken into account, it becomes clear that the ITO, as reduced and amplified, could not possibly have afforded reasonable and probable grounds to believe that the accused possessed child pornography and that evidence of that crime would be found on his computer at the time the warrant was sought or *at any time*.

[45] First, it is necessary to excise several misleading passages in the ITO that suggested Mr. Hounjet had actually viewed illegal pornography on the computer, rather than suspiciously-labelled bookmarks ("Favourites"). In particular, para. 5 of the ITO, the first to adduce specific facts in support of the application, contains two glaring and misleading inaccuracies. It states, first, that "[o]nce on the computer HOUNJET observed 'Lolita Porn' on the screen", and then that Mr. Hounjet "returned the next day to find the porn removed".

[46] The clear implication of these assertions is that Mr. Hounjet in fact saw "Lolita porn" (pornography involving young girls) on the screen and that he determined that this pornography was subsequently removed from the computer. But Mr. Hounjet saw nothing of the sort. As is clear from the *voir dire*, all he saw were two links labelled "Lolita Porn" and "Lolita XXX" in the "Favourites" menu of the Internet browser. "Favourites" or bookmarks are nothing more than "menu entries" that serve as shortcuts that provide easy access to an Internet site.

[47] Justice Deschamps finds (at para. 155) that "[t]here could be no confusion about what was seen". I respectfully disagree. Nowhere does the ITO disclaim the clear statement in para. 5 that Mr. Hounjet saw "Lolita Porn" and that "the porn" was subsequently removed. While para. 10 does

specify that Mr. Hounjet saw "Lolita Porn" and "Lolita XXX" *icons*, the last sentence of that very paragraph perpetuates the impression that *actual* child pornography (rather than links) were seen: It asserts that when Mr. Hounjet arrived the next day "all the child porn off the computer was gone".
[48] There is no reasonable basis for assuming that the justice of the peace would have understood these clear and misleading statements to refer exclusively to the icons mentioned in para.
10. The natural reading of the ITO is that pornographic images of children were actually seen on the computer. This is an entirely false claim, and these statements must therefore be excised from the ITO.

[49] Aside from false statements, the ITO in several places gave an incomplete and misleading account of the facts, in contravention of the informant's duty to make full and frank disclosure of all material information.

[50] For example, the *voir dire* revealed that the two bookmarks described in the ITO — the bookmarks labelled "Lolita Porn" and "Lolita XXX" — were "just scattered through the favourites" among additional links pointing to "regular adult material" (Testimony of Adrian Hounjet at the *voir dire*, A.R., at pp. 98-100). This is not mentioned at all in the ITO.

[51] Moreover, the only pornographic image that Mr. Hounjet actually did see — an image on the accused's computer desktop or Internet homepage — was perfectly legal adult pornography. The failure to mention these facts creates a misleading impression that the accused was particularly inclined towards child pornography or exclusively seeking it out. [52] Once it is clearly understood that the suspicious "Favourites" were in fact anomalies or exceptions, found together with much more material that was undisputedly legal, the inference that the accused possessed illegal images — or that evidence of criminal possession would be found upon a search of the computer — becomes significantly less compelling.

[53] Similarly, the ITO placed great emphasis on the presence of a "web-cam pointing towards [children's] toys", and noted also that "[t]he client was alone in the house with a three year old child" (ITO, at para. 5). Indeed, these statements appear in the very first substantive paragraph of the ITO. Later in the ITO, one learns that the webcam was not hooked up to the computer but was rather plugged into a VCR that recorded to videotape (at para. 10).

[54] The descriptions of the webcam and its placement are juxtaposed immediately alongside the descriptions of the suspicious "Favourites" and the claims that Mr. Hounjet had "observed 'Lolita Porn'". The ITO thus invited the justice of the peace to make an unwarranted connection between the two "Lolita" bookmarks and the webcam trained at the children's play area. Read as a whole, the ITO could thus be understood to allege that the accused had made and possessed his own illegal pornography, in addition to possessing images from the Internet on his computer.

[55] The informant's narrative would have appeared much less sinister — and much less supportive of the claim that the accused possessed child pornography — had the ITO included a number of additional facts known to the police.

[56] First, the three-year old child mentioned (but not identified) in the ITO was in fact the

accused's daughter. Second, the ITO stated that the accused was alone in the house with the girl, but failed to mention that his wife lived with them. Third, the ITO failed to mention that the child was fully clothed, that there was no evidence of abuse, that the computer room had a child gate and appeared to double as a playroom for the child, and that the child was playing with the scattered toys in the middle of the room when Mr. Hounjet arrived, before being taken out of the room by the accused (A.R. at pp. 206-10).

[57] These omitted facts all tend to undermine suspicions about the accused. Once they are added to the picture, it seems much more plausible that the accused was simply using the VCR and webcam to videotape his young daughter at play for posterity's sake, rather than for any purpose connected to child pornography.

[58] In failing to provide these details, the informant failed to respect his obligation as a police officer to make full and frank disclosure to the justice. When seeking an *ex parte* authorization such as a search warrant, a police officer — indeed, any informant — must be particularly careful not to "pick and choose" among the relevant facts in order to achieve the desired outcome. The informant's obligation is to present *all material facts, favourable or not*. Concision, a laudable objective, may be achieved by omitting irrelevant or insignificant details, but not by material non-disclosure. This means that an attesting officer must avoid incomplete recitations of known facts, taking care not to invite an inference that would not be drawn or a conclusion that would not be reached if the omitted facts were disclosed.

[59] The relevant question here is whether the ITO was misleading, not whether it was

intentionally misleading. Indeed, in the Court of Queen's Bench, the judge who had the benefit of observing the Crown's witnesses on the *voir dire* found no deliberate attempt to mislead. That conclusion should not be disturbed. It is nonetheless evident that the police officer's selective presentation of the facts painted a less objective and more villainous picture than the picture that would have emerged had he disclosed all the material information available to him at the time.

[60] The facts originally omitted must be considered on a review of the sufficiency of the warrant application. In *Araujo*, the Court held that where the police make good faith errors in the drafting of an ITO, the warrant authorization should be reviewed in light of amplification evidence adduced at the *voir dire* to correct those mistakes. Likewise, where, as in this case, the police fail to discharge their duty to fully and frankly disclose material facts, evidence adduced at the *voir dire* should be used to fill the gaps in the original ITO.

V

[61] The admissibility of the evidence obtained pursuant to the search and seizure of the appellant's computer depends on two constitutional considerations. The first is whether the search and seizure were unreasonable, within the meaning of s. 8 of the *Charter*; the second is whether admission of the evidence thereby obtained would bring the administration of justice into disrepute, and should therefore be excluded pursuant to s. 24(2).

[62] The second question is only reached, of course, if the first is resolved in the appellant's favour. And that depends on whether the ITO, stripped of its erroneous and tendentious assertions,

and amplified as indicated, provides sufficient credible and reliable evidence to have permitted the justice of the peace to find reasonable and probable grounds to believe both that the appellant was in culpable possession of child pornography and that evidence of that crime would be found in his computer.

[63] Essentially, only two inferential paths could have led the justice to conclude that the warrant should issue: (1) the two suspicious bookmarks; (2) the claims about the propensity of certain "types of offenders" to hoard images, combined with reason to believe that the accused is of that "type". In my view, both paths lead instead to an evidentiary dead end: they culminate in suspicion and conjecture, never reaching the mandatory threshold of reasonable and probable grounds to believe.

[64] The presence of the two "Lolita" links in the Favourites certainly supports a reasonable inference that the accused browsed a Website that contained explicit images of females under the age of 18. And it is not unreasonable to infer from the mere presence of the links on the appellant's computer, in the absence of evidence to the contrary, that they were knowingly added by him.

[65] This does not suffice, however, to establish possession. First, as earlier explained, merely browsing a website or viewing images onscreen does not constitute possession. Neither does creating a bookmark on one's computer establish possession over the content of the Website: bookmarks merely provide quick and easy *access* to the indicated Websites. Indeed, clicking on a bookmark may simply disclose that material previously on the Website has been removed; that material previously absent has been added; that the Website address is no longer valid — or that the

Website no longer exists at all.

[66] Accordingly, in order to commit the offence of possession (as opposed to the offence of accessing), one must *knowingly acquire the underlying data files and store them in a place under one's control*. The presence of the icons might arouse suspicions regarding possession, but it does not alone support a reasonable inference that the appellant not only accessed the website and knowingly viewed illegal images located there, but also took the underlying data file into his control by saving it to the hard drive, or otherwise.

[67] Even if one takes the broader view that possession is complete on merely viewing images on-screen, other facts in the ITO preclude the possibility of inferring from the icons alone that evidence of the crime would be found in the appellant's computer.

[68] Specifically, the ITO states that on the day after the icons were viewed, the computer's hard drive was "formatted". On the *voir dire*, it was confirmed that this meant that the entire contents of the hard drive were deleted. Not only would the suspicious links have thus been erased, but illegal image files in the computer and any files evidencing past access to Websites containing illegal images (such as browser histories or cache files) would also have been removed. Normally, moreover, the greater the lapse of time after a hard drive has been formatted, the more likely it will be impossible to recover the former contents of the drive using forensic tools. In this case, four months had passed. And, in any event, the nature of "formatting" and data retention on computer drives was not sufficiently described in the ITO to permit issuance of the warrant on these grounds.

[69] To conclude that evidence of possession would be found four months after the hard drive was erased, one must therefore accept either that the accused had made external copies of illegal images present in the computer before formatting its hard drive or that he acquired additional illegal images after the formatting.

[70] Both possibilities require drawing inferences based on the likely behaviour of the accused. The ITO seeks to establish the necessary inference on the basis of unsupported generalizations about the propensities of certain "types of offenders" to hoard and copy illegal images. The ITO suggests that the accused is a person of that "type" and that, as a result, copies of the images would remain on the computer.

[71] In my view, the ITO does not establish either the veracity of the generalization about the alleged "type of offender", nor that the accused is in fact the "type" to which the generalization might have applied.

[72] More specifically, the ITO makes two statements about the "propensities" of offenders. It first states that "these type[s] of offenders are habitual and will continue their computer practices with child pornography" (ITO, at para. 12). This claim is attributed to Corporal Boyce of the RCMP Technological Crime Unit. The ITO also claims that "offenders treasure collections on their computer and like to store them and create backup's (*sic*) in case they loose (*sic*) it. Discs and floppy disks are used for this purpose. Offenders will typically sort information and store pictures on different file names to catagorize (*sic*) them." (ITO, at para. 13). This statement is attributed to Constable Huisman of the Saskatoon Police Service Vice Unit. [73] The main difficulty with these generalizations about certain "types of offenders" is that they are entirely devoid of meaningful factual support. The ITO contains no evidentiary material in this regard, even anecdotal, apart from the bald assertion of the two police officers. Furthermore, there is virtually nothing to describe, let alone establish, the expertise of the officers to whom the claims are attributed. The only information provided in the ITO consists in the officers' names, positions, and places of work. This is surely an insufficient evidentiary basis to enable a justice of the peace, hearing an application *ex parte*, to determine that the generalization is sufficiently credible or reliable to form the basis for a finding of reasonable and probable grounds.

[74] The amplification evidence presented on the *voir dire* is of little assistance to the Crown. The failure to provide evidence of the officers' expertise does not seem to be a mere "minor, technical error" that, in light of *Araujo*, could be corrected with evidence adduced at the *voir dire*. In any event, it appears from this evidence that Cst. Ochitwa, the officer who prepared the ITO, believed Cst. Huisman to be an expert in crimes involving child pornography only on the basis of a recommendation from a prosecutor, his own impressions from talking to Cst. Huisman, and his understanding that Cst. Huisman had previously worked on unspecified "child exploitation offences". Cst. Ochitwa's testimony does not mention any knowledge of the relevant experience that Cst. Huisman may have had or the basis for his opinions about the proclivities of child pornography offenders (Testimony of Cst. Ochitwa, A.R., at pp. 158-59 and 192-94).

[75] The evidence presented at the *voir dire* with respect to Cpl. Boyce's statements is more problematic still. Cst. Ochitwa testified that he approached Cpl. Boyce in order to obtain

information about "how computers operate" because "[Cpl. Boyce] was involved with the term (*sic*) technological crime". Cpl. Boyce thus appears to have been sought out as an expert on *computer technology*, not the habits of child pornography offenders. While Cst. Ochitwa was aware that Cpl. Boyce worked in the Technological Crimes Unit and knew what his duties were there — investigating crimes involving computers — there is no indication at all whether or how his work in that unit formed the basis for his opinions about child pornography offenders (Testimony of Cst. Ochitwa, A.R., at pp. 157-58 and 191-92).

[76] Perhaps even more troubling than the paucity of information as to the basis for the officers' opinions is the fact that the class of persons to whom specific proclivities are attributed is defined so loosely as to bear no real significance. Both officers speak about the propensities of undefined "types of offenders" or simply "offenders".

[77] While it is clear from the context that the officers are referring to some variety of child pornography offenders, it cannot be assumed, without evidence, that broad but meaningful generalizations can be made about all persons who commit (or are suspected of committing) child pornography offences. For example, a person with an exclusive interest in child pornography is surely of a different "type" than a person who is primarily or exclusively interested in legal adult images, but has nevertheless downloaded a small number of illegal images. Similarly, a person who seeks out pornographic images of young children or infants is likely a different "type" than a person who views images of teenagers under the age of 18.

[78] These people all commit child pornography offences, but the "propensities" of one type
may well differ widely from the "propensities" of others. There is no reason to believe, on the basis of the information in the ITO, that *all* child pornography offenders engage in hoarding, storing, sorting, and categorizing activity. And there is nothing in the ITO that indicates which specific subset of these offenders does generally engage in those activities.

[79] To permit reliance on broad generalizations about loosely-defined classes of people is to invite dependence on stereotypes and prejudices in lieu of evidence. I am thus unable to agree with Justice Deschamps (at para. 162) that the ITO's claims in this regard could properly be relied on by the justice.

[80] Justice Deschamps supports her reliance on claims about the behaviour of "types of offenders" by citing child pornography cases in which courts, in her view, have accepted the tendency of certain kinds of child pornography offenders to collect many images and store them over long periods of time (para. 162). These decisions are rather in favour of the conclusion that an evidentiary basis is required to support a finding as to the characteristics or propensities of child pornography offenders.

[81] That some child pornography offenders do seek out and hoard illegal images is, of course, neither surprising nor helpful in determining whether reasonable and probable grounds exist in a particular case. Still, it is not the role of courts to establish by judicial fiat broad generalizations regarding the "proclivities" of certain "types" of people, including offenders. Matters of this sort are best left to be established by the Crown, according to the relevant standard — in this case, reasonable and probable grounds for belief. As suggested earlier, moreover, courts must be particularly wary of

endorsing such generalizations when, as in this case, the crime alleged is the subject of intense emotional responses and widespread condemnation, and the temptation to rely on stereotype rather that evidence is therefore especially dangerous and strong.

[82] An evidentiary basis is required as well for a finding of reasonable and probable grounds to believe that the alleged offender belongs to the class of child pornography offenders whose characteristics or propensities are mentioned in the ITO. This view of the law was adopted in *R. v. Fawthrop*, (2002), 161 O.A.C. 350, the only Canadian appellate decision cited by Justice Deschamps. My colleague finds in that decision support for her suggestion that general opinions on the propensity of child pornography offenders to collect and hoard child pornography material can give rise to reasonable and probable grounds for issuing search warrants. With respect, I read *Fawthrop* differently. As noted earlier, *Fawthrop* affirms the need for evidence both as to characteristics of an identified class of child pornography offenders, and as to the offender's membership in that class.

[83] As Borins J.A., speaking for the majority of the Ontario Court of Appeal, explained in *Fawthrop* (at para. 42):

In my view, the trial judge's finding, based on the testimony of Det. Const. Pulkki, that the police were engaged in a "fishing expedition" for items of child pornography leads to the conclusion that the breach of the appellant's s. 8 *Charter* rights was serious. It appears from the record that after she interviewed A.Y. and members of her family, Det. Const. Pulkki suspected that the appellant was a pedophile, which led her to further suspect that he might possess items of child pornography. To be fair to her, she realized that her suspicion was insufficient to enable her to obtain a warrant. She was aware that it was necessary that she have reasonable grounds to believe that child pornography would be located in the appellant's home. She sought the opinion of Dr. Collins in the hope that it would tip the scales from suspicion to reasonable grounds. As the trial judge recognized, the opinion of Dr. Collins failed to do so. He recognized the fatal flaw in the opinion. Although Dr. Collins opined that it was not uncommon for pedophiles to collect items of child pornography, he was unable to form an opinion as to whether the appellant was a pedophile. Without that link, Det. Const. Pulkki was in the same position as she had been before she contacted Dr. Collins. All she had was a suspicion that the appellant might be in possession of child pornography. ... This resulted in an unauthorized search for those items by means of what the trial judge correctly labelled a "fishing expedition". This is what the search warrant process is meant to prevent.

In the result, the evidence seized under the warrant was excluded pursuant to s. 24(2) of the *Charter*.

[84] In short, in most of the cases cited by my colleague, the original warrant application included relatively detailed descriptions of the habits of a specific class of child pornography offender. They thus provided evidence sufficient to establish a credible profile of a class of child pornography collectors and their typical behaviours, and a proper factual foundation for concluding that the alleged offender belonged to that class. This is not our case.

[85] Here, even if the impugned generalizations are accepted, the ITO as amplified does not reasonably permit the inference that the accused was the "type of offender" who sought out illegal pornography and stored it. This requirement was well explained in *United States v. Weber*, 923 F.2d 1338 (9th Cir. 1990)), at p. 1345: "[I]f the government presents expert opinion about the behavior of a particular class of persons, for the opinion to have any relevance, the affidavit must lay a foundation which shows that the person subject to the search is a member of the class".

[86] Two suspiciously-labelled links in the "Favourites" menu do not suffice to characterize a person as an habitual child pornography offender of the type that seeks out and hoards illegal images. Indeed, the fact that the bulk of the pornographic material that Mr. Hounjet observed at the accused's house was perfectly legal adult pornography suggests that the accused did not have a "pronounced" interest in child pornography at all, contrary to my colleague's assertion (paras. 177 and 179).

[87] Also, and again with respect, the cases my colleague relies on (at para. 173) do not support the notion that a warrant can be issued months after a person might have merely viewed child pornography. For example, in *United States v. Terry*, 522 F.3d 645 (6th Cir. 2008), the warrant was issued on a probable cause finding that the accused *had in fact saved child pornography on his computer five months earlier*. Also, the Prince Edward Island Court of Appeal in *R. v. Graham*, 2008 PESCAD 7, 277 Nfld. & P.E.I.R. 103, neither upheld the warrant nor affirmed the trial judge's finding as to the effect of the passage of time.

[88] More broadly, Justice Deschamps may be understood to permit reasonable and probable grounds for belief to rest on evidence that has only a tenuous relation to the crime in question — possessing illegal child pornography.

[89] For example, my colleague is of the view that the presence of the webcam, which was functioning effectively as a camcorder recording to a VCR, "showed that [the accused] was interested in reproducing images, accumulating such material, and keeping it for his future use", showed that the accused "was in the habit of reproducing and saving images and had a propensity to pornography and more specifically to child pornography" (para. 179). With respect, neither the legal nor the logical relevance of these considerations is apparent to me.

[90] While it may be true that the accused was adept at recording videotapes and storing the tapes for future use — as is nearly everyone who owns a camcorder — this says absolutely nothing about his propensity to store a completely different kind of image (child pornography), in a completely different medium (a computer, as opposed to videotape), acquired in a completely different manner (downloading, as opposed to filming).

[91] The mere fact that a person collects, reproduces, or stores *anything* — music files, letters, stamps, and so forth — hardly supports an inference that he or she is of the type to hoard illegal images. To draw that inference here is to speculate impermissibly. At its highest, the proposed inference might provoke suspicion in some. And, as a matter of law, suspicion is no substitute for reasonable and probable grounds to believe either that the appellant committed the alleged offence or that evidence of the offence would be found in his computer.

[92] Nor do I consider that the accused's conduct after the visit — tidying up the room and formatting the hard drive — supports the conclusion that the accused was the sort of person to seek out and hoard child pornography.

[93] Justice Deschamps contends that these actions were evidence of a "desire not to arouse suspicion with respect to his reproduction of images or his computer practices" and that the conduct created "a credibly based probability that the appellant was in the habit of reproducing and saving images and had a propensity to pornography, and more specifically to child pornography" (para. 179). [94] In my view, there is an obvious and innocent explanation for this conduct that is at least as plausible: The accused might well have tidied up and formatted his computer simply to avoid further embarrassment from having an outsider see the disorderly state of his home and the evidence of his consumption of pornography on his computer. Again, the accused's conduct might raise suspicions, but it establishes nothing more.

[95] In short, as mentioned at the outset, the ITO in this case is reduced by scrutiny to two links in the browser's list of "Favourites" — links that were known to have been erased four months earlier. At best, this may be a ground for suspicion, but surely the deleted links afford no reasonable and probable grounds to believe that the appellant was in possession of child pornography, and still less that evidence of that crime would be found upon a search of his computer.

[96] Once the material facts omitted from the ITO are taken into consideration, it is apparent that none of the other evidence in the ITO — principally the presence of the webcam and the claims about propensities of unspecified "types of offenders" — can elevate mere suspicion into sufficient grounds for a warrant.

[97] Because the warrant should not have issued, the subsequent search violated s. 8 of the *Charter*.

VI

[98] To determine whether the evidence obtained as a result of the illegal search should be

excluded under s. 24(2), we are bound to apply the test recently set out in *Grant*, at para. 71:

[U]nder s. 24(2), a court must assess and balance the effect of admitting the evidence on society's confidence in the justice system having regard to: (1) the seriousness of the *Charter*-infringing state conduct (admission may send the message the justice system condones serious state misconduct), (2) the impact of the breach on the *Charter*-protected interests of the accused (admission may send the message that individual rights count for little), and (3) society's interest in the adjudication of the case on its merits. The court's role on a s. 24(2) application is to balance the assessments under each of these lines of inquiry to determine whether, considering all the circumstances, admission of the evidence would bring the administration of justice into disrepute.

I shall consider these three factors in turn.

[99] First, the *Charter*-infringing state conduct in this case was the search of the accused's home and the seizure of his personal computer, his wife's laptop computer, several videotapes, and other items. The search and seizure were unwarranted, but not warrantless: they were conducted pursuant to a search warrant by officers who believed they were acting under lawful authority. The executing officers did not wilfully or even negligently breach the *Charter*. These considerations favour admission of the evidence. To that extent, the search and seizure cannot be characterized as particularly egregious.

[100] The opposite is true on considering the ITO upon which the warrant was obtained. The officer who *prepared* the ITO was neither reasonably diligent nor mindful of his duty to make full and frank disclosure. At best, the ITO was improvidently and carelessly drafted. Not only did the ITO fail to specify the correct offence (assessing rather than possession of child pornography); it was also drafted in a misleading way, resulting in the issuance of a warrant on insufficient grounds. While the trial judge found no deliberate attempt to mislead, no attesting officer, acting reasonably, could have failed to appreciate that repeated references to "'Lolita Porn' on the screen" and to the deletion of "all the child porn off the computer" would cause most readers — and, more particularly, the issuing justice — to believe there was evidence that child pornography was actually viewed on-screen by the witness Hounjet.

[101] Similarly, the officer should have known — if he in fact did not — that the immediate juxtaposition of these misleading statements and the incomplete description of the "web-cam pointing towards toys" would be unjustifiably inflammatory.

[102] The repute of the administration of justice is jeopardized by judicial indifference to unacceptable police conduct. Police officers seeking search warrants are bound to act with diligence and integrity, taking care to discharge the special duties of candour and full disclosure that attach in *ex parte* proceedings. In discharging those duties responsibly, they must guard against making statements that are likely to mislead the justice of the peace. They must refrain from concealing or omitting relevant facts. And they must take care not to otherwise exaggerate the information upon which they rely to establish reasonable and probable grounds for issuance of a search warrant.

[103] We are bound to accept the trial judge's finding that there was no deliberate misconduct on the part of the officer who swore the Information. The repute of the administration of justice would nonetheless be significantly eroded, particularly in the long term, if such unacceptable police conduct were permitted to form the basis for so intrusive an invasion of privacy as the search of our homes and the seizure and scrutiny of our personal computers.

[104] I turn in that light to the second factor set out in *Grant*: The impact of the breach on the *Charter*-protected interests of the accused. The intrusiveness of the search is of particular importance in this regard. Our concern here is with the search of the appellant's home, in itself a serious breach of the appellant's rights under s. 8 of the *Charter*. But there is more. The infringement in this case involved a search of the appellant's personal computer — and his wife's laptop computer as well. In passing, I recall here the Informant's failure to mention that the appellant lived with his wife. This not only cast a dark light in the appellant's presence alone with their child — perfectly understandable in the circumstances — but may also explain why the laptop, which was in fact not his, was seized and presumably scrutinized as well.

[105] As I mentioned at the outset, it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers 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, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.

[106] It is therefore difficult to conceive a s. 8 breach with a greater impact on the *Charter*-

protected privacy interests of the accused than occurred in this case.

[107] I turn, finally, to the third factor to be weighed under s. 24(2) of the *Charter* — society's interest in adjudication of the case on its merits. Here, exclusion of the evidence obtained in the search would leave the prosecution with essentially no case against the accused. It would thus seriously undermine the truth-seeking function of the trial, a factor that weighs against exclusion (*Grant*, at paras. 79-83).

[108] In balancing these considerations, we are required by *Grant* to bear in mind the longterm and prospective repute of the administration of justice, focussing less on the particular case than on the impact over time of admitting the evidence obtained by infringement of the constitutionally protected rights of the accused.

[109] In my view, the repute of the administration of justice will be significantly undermined if criminal trials are permitted to proceed on the strength of evidence obtained from the most private "place" in the home on the basis of misleading, inaccurate, and incomplete Informations upon which a search warrant was issued.

[110] Justice is blind in the sense that it pays no heed to the social status or personal characteristics of the litigants. But justice receives a black eye when it turns a blind eye to unconstitutional searches and seizures as a result of unacceptable police conduct or practices.

[111] The public must have confidence that invasions of privacy are justified, in advance, by a

genuine showing of probable cause. To admit the evidence in this case and similar cases in the future would undermine that confidence in the long term.

[112] I am persuaded for all of these reasons that admitting the illegally obtained evidence in this case would bring the administration of justice into disrepute.

[113] I would therefore exclude that evidence and, since there was no possibility that the accused could have been convicted in the absence of the evidence, I would allow the appeal, quash the appellant's conviction and enter an acquittal in its place.

The reasons of Deschamps, Charron and Rothstein JJ. were delivered by

DESCHAMPS J. —

[114] Internet and computer technologies have brought about tremendous changes in our lives. They facilitate the communication of information and the exchange of material of all kinds and forms, with both legal and illegal content, and in infinite quantities. No one can be unaware today that these technologies have accelerated the proliferation of child pornography because they make it easier to produce, distribute and access material in partial anonymity: Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (2008), at pp. 1-8. Not only do these technologies increase the availability of child pornography; they also raise new challenges, as the criminal law must be adapted to apply to the making, distribution, and possession of such material, while the resulting offences must be investigated in a manner consistent with fundamental

rights.

[115] The case at bar raises one such challenge. The appellant contends that the search of his computer breached his rights under s. 8 of the *Canadian Charter of Rights and Freedoms* and that the evidence found on the computer should therefore be excluded and an acquittal entered on a charge of possession of child pornography (s. 163.1(4) *Criminal Code*, R.S.C. 1985, c. C-46). For the reasons that follow, I conclude that the reviewing judge did not err in upholding the decision to issue the warrant. Consequently, there is no need to address s. 24(2) of the *Charter*. I would dismiss the appeal.

I. Facts

[116] In 2002, Adrian Hounjet worked as a computer technician for the Keewatin Career Development Corporation. He was trained to repair computers and install high-speed Internet connections. At the time, he was also responsible for creating software to prevent school children from visiting pornographic sites and for keeping it up to date. He had accordingly accessed such sites in order to build a database to support that software, and he was familiar with the vocabulary of child pornography.

[117] The appellant had ordered a high-speed Internet connection from SaskTel. On September 5, 2002, Mr. Hounjet arrived unannounced at the appellant's residence in La Ronge to perform the installation. The appellant lived with his wife and two children, aged three and seven, but was alone that day with his three-year-old daughter. He looked surprised, but allowed Mr. Hounjet in.

[118] Several things he saw, taken together, struck Mr. Hounjet "as a little bit odd". The computer was located in a spare bedroom where the three-year-old child was playing with toys on the floor. He saw that the accused already had access to the Internet, probably by means of a dial-up service. When he opened the Web browser, he noticed several links to both adult and child pornography in the taskbar's "favourites" list, including two that were labelled "Lolita Porn" and "Lolita XXX". He also saw a pornographic image, but he could not remember afterwards if it was on the browser's home page or on the computer desktop. The image was, in his words, "pretty graphic" and he wondered if the appellant's wife "let him view and keep it on as their desktop". From his experience in building the database for the anti-pornography software, Mr. Hounjet recognized "Lolita" as a term associated with child pornography. While working on the computer, he also noticed home videos and, on a tripod, a webcam that was connected to a videotape recorder and was pointed at the toys and the child instead of being aimed, as webcams usually are, at the computer user's seat. The fact that the camera was pointed at the child would not normally have struck him as odd, but in light of the links on the computer to pornography, it troubled him. He did not click on the links to access the websites at that time.

[119] Unable to finish his work on that day, Mr. Hounjet had to return the following morning, on September 6, 2002. He then noticed that everything had been "cleaned up": the child's toys had been placed in a box, the videotapes could no longer be seen, the webcam was pointed at the computer user's chair and the computer had been "formatted". (The only reference in the record to the meaning of the word "formatted" is in Mr. Hounjet's statement to the police. When asked what

it meant, he answered: "The whole thing gets erased. The icons were gone" (A.R., at p. 209).)

[120] Uneasy about what he had seen at the appellant's residence and having noted the names of some of the links in the "favourites" list, Mr. Hounjet, after returning to his place of work, accessed the websites to which they were related. He saw there what he believed to be child pornography. He testified that some of the people in the photographs looked "younger than 18 and 15 or 14 or 13 even".

[121] Mr. Hounjet continued to think about these events and eventually, in November 2002, discussed them with his mother, a former social worker. She in turn contacted the social services office in La Ronge on November 14, 2002. At that time, Mr. Hounjet's concerns related to the child's safety. On November 15, 2002, he went to the social services office and reported what he had seen. The social worker, Valerie Fosseneuve, contacted the Royal Canadian Mounted Police ("RCMP") on November 18, 2002 and reported the information received from Mr. Hounjet to Cpl. Susan Kusch. Cpl. Kusch then contacted Cpl. Mike Boyce of the RCMP's Technological Crime Unit in Regina. Cpl. Boyce confirmed what Mr. Hounjet had said concerning the names of the websites, stating that "'Lolita' is an underage porn site that primarily deals with children 14 years old and under". About a week later, Cst. Mark Ochitwa was assigned to investigate the matter.

[122] Some time elapsed before the investigation really started. Cst. Ochitwa was out of the country for more than a week after being assigned to the investigation. When he tried to contact Mr. Hounjet on December 17, the latter was away until Christmas, and then Cst. Ochitwa was on holiday until the beginning of the new year. Cst. Ochitwa finally obtained Mr. Hounjet's statement

on January 8, 2003. After the interview, he consulted Cpl. Boyce, who he knew had experience investigating crimes involving computers and technological devices. Cpl. Boyce provided information about "media, storage media, computers, and specifically about this crime that these images are and would remain on a computer". He also contacted a Crown Attorney in Regina, who suggested that he speak with Cst. Randy Huisman of the Saskatoon Police Service, who had experience investigating child exploitation offences. Cst. Huisman informed him that "these type of persons treasure collections, child pornography collections, similar to that of a coin collector or a stamp collector, and they categorize and catalogue these images and ... their material". Cst. Ochitwa also verified whether an active Internet connection was still being provided to the appellant's residence. He then drafted an information to obtain a search warrant ("ITO"). It is reproduced as an appendix to these reasons, but the salient parts will be cited when most relevant.

[123] A search warrant was issued on January 10, 2003, and the search was carried out the same day. Pornographic pictures involving children were found on the computer, computer disks and/or floppy disks. The appellant was charged with possession of child pornography contrary to s. 163.1(4) of the *Criminal Code*. At trial, the appellant challenged the validity of the search warrant under s. 8 of the *Charter* and sought to have the evidence from the computer excluded.

[124] On September 15, 2005, the trial judge, Rothery J., conducted a *voir dire* to determine whether the evidence was admissible. She dismissed the appellant's challenge of the search warrant (2005 SKQB 381 and 381A, 272 Sask. R. 282). The appellant was convicted and was sentenced to an 18-month conditional sentence. On appeal, the majority confirmed the trial judge's ruling that the search warrant was valid (2008 SKCA 62, 310 Sask. R. 165). Richards J.A. dissented.

He would have allowed the appeal, excluded the evidence and entered an acquittal.

[125] In this Court, the appellant essentially adopts Richard J.A.'s dissent. He argues that the search warrant was invalid because there were no reasonable grounds. He contends that the evidence found on his computer should be excluded. This would result in an acquittal. The Crown submits that there were reasonable grounds justifying the issuance of the warrant. In the alternative, if the warrant was improperly issued, the respondent contends that the evidence should be admitted under s. 24(2) of the *Charter* and the conviction affirmed.

II. <u>Analysis</u>

[126] The search warrant in this case was issued pursuant to the general search and seizure provision, s. 487 of the *Criminal Code*. The standard to be met for the authorization of a search is found in the wording of the section, which reads in part as follows:

487. (1) A justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

(a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,

(b) anything that there are <u>reasonable grounds to believe will afford evidence with</u> respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,

(c) anything that there are reasonable grounds to believe is intended to be used for

the purpose of committing any offence against the person for which a person may

be arrested without warrant, or ...

[127] The concept of "reasonable grounds to believe" has been considered by this Court on numerous occasions. The most frequently cited formulation of the standard as applicable to the context of a search was articulated by Wilson J. in *R. v. Debot*, [1989] 2 S.C.R. 1140, at p. 1166:

The question as to what standard of proof must be met in order to establish reasonable grounds for a search may be disposed of quickly. I agree with Martin J.A. that the appropriate standard is one of "reasonable probability" rather than "proof beyond a reasonable doubt" or "*prima facie* case". The phrase "reasonable belief" also approximates the requisite standard.

See also Baron v. Canada, [1993] 1 S.C.R. 416.

[128] The genesis of the addition of the notion of probability to the concept of reasonable grounds can be traced to *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 167, where Dickson J. (as he then was) stated that the Canadian "reasonable grounds to believe" requirement was identical to the "probable cause" threshold for a search warrant set out in the U.S. *Bill of Rights*. The Court described the requirement as "the point where credibly-based probability replaces suspicion" (p. 167). What Dickson J. was in fact trying to do in *Hunter* was to establish a criterion that elevated the grounds for a search beyond subjective belief and mere suspicion (at p. 167):

The problem is with the stipulation of a reasonable belief that evidence <u>may</u> be uncovered in the search. Here again it is useful, in my view, to adopt a purposive approach. The purpose of an objective criterion for granting prior authorization to conduct a search or seizure is to provide a consistent standard for identifying the point at which the interests of the state in such intrusions come to prevail over the interests of the individual in resisting them. To associate it with an applicant's reasonable belief that relevant evidence <u>may</u> be uncovered by the search, would be to define the proper standard as the <u>possibility</u> of finding evidence. This is a very low standard which would validate intrusion on the basis of suspicion, and authorize fishing expeditions of considerable latitude. It would tip the balance strongly in favour of the state and limit the right of the individual to resist, to only the most egregious intrusions. I do not believe that this is a proper standard for securing the right to be free from unreasonable search and seizure.

Anglo-Canadian legal and political traditions point to a higher standard. The common law required evidence on oath which gave "strong reason to believe" that stolen goods were concealed in the place to be searched before a warrant would issue. Section 443 of the *Criminal Code* authorizes a warrant only where there has been information upon oath that there is "reasonable ground to believe" that there is evidence of an offence in the place to be searched. The American *Bill of Rights* provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation...." The phrasing is slightly different but the standard in each of these formulations is identical. The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. [Emphasis in the original.]

[129] Determining whether evidence gives rise to a "credibly-based probability" does not involve parsing the facts or assessing them mathematically. Rather, what the judge must do is identify credible facts that make the decision to authorize a search reasonable in view of all the circumstances. I therefore agree with the non-technical, common-sense approach taken by Rehnquist J. (as he then was) in *Illinois v. Gates*, 462 U.S. 213 (1983):

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a

fair probability that contraband or evidence of a crime will be found in a particular place. [p. 238]

[130] Where, as here, a court reviews the validity of a search warrant, it does not ask whether it would have reached the same decision as the authorizing judge. It merely determines whether there was credible evidence on which the decision could be based. This exercise is not a *de novo* review. In *R. v. Garofoli*, [1990] 2 S.C.R. 1421, at p. 1452, Sopinka J., writing for the majority, stated:

The reviewing judge does not substitute his or her view for that of the authorizing judge. If, based on the record which was before the authorizing judge as amplified on the review, the reviewing judge concludes that the authorizing judge could have granted the authorization, then he or she should not interfere. In this process, the existence of fraud, non-disclosure, misleading evidence and new evidence are all relevant, but, rather than being a prerequisite to review, their sole impact is to determine whether there continues to be any basis for the decision of the authorizing judge.

This test was applied to the review of the authorization of a search in *R. v. Grant*, [1993] 3 S.C.R. 223, and was reiterated by LeBel J. in *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 54:

[T]he test is whether there was reliable evidence that might reasonably be believed on the basis of which the authorization could have issued, not whether in the opinion of the reviewing judge, the application should have been granted at all by the authorizing judge. [Emphasis deleted.] [131] The reviewing judge considers the evidence presented in the ITO, as amplified at the review hearing. The ITO must contain a full and frank disclosure of the relevant material facts, and no attempt should be made to trick those who read it (*Araujo*, at paras. 46-47). As LeBel J. stated, "erroneous information is properly excised.... [However, where such] information results from a simple error and not from a deliberate attempt to mislead the authorizing judge, amplification may be in order" (*Araujo*, at para. 57). The onus is on the accused to demonstrate that the ITO is insufficient: *Quebec (Attorney General) v. Laroche*, 2002 SCC 72, [2002] 3 S.C.R. 708, at para. 68.

[132] When the review hearing takes place during a *voir dire*, the point at which the judge determines whether the warrant is valid is closer in time to the determination of guilt. However, this proximity must not result in a co-mingling of these distinct issues or a conflation of the distinct burdens of proof the Crown must discharge. In my respectful opinion, co-mingling the issues and conflating the burdens of proof is precisely what my colleague Fish J. is doing. We are not asked to determine whether the evidence is sufficient to establish guilt. What is at issue is "whether there was any basis upon which the authorizing judge could be satisfied that the relevant statutory preconditions existed": *R. v. Pires*, 2005 SCC 66, [2005] 3 S.C.R. 343, at para. 30.

[133] In the case at bar, the appellant contends that the presence of the links in his "favourites" list was not "sufficient to establish reasonable grounds [to believe] that (his) computer would contain child pornography". He argues that no child pornography had been seen on the computer and that, considering the delay, there was no reasonable probability that the computer and the alleged "child pornography" would still be in his residence. The appellant also challenges

allegations in the ITO on the bases that they are incomplete or false, or that they contain boilerplate statements. In addition, he argues that the opinions of Cpl. Boyce and Cst. Huisman have no probative value and that, in view of the delay, there were no reasonable grounds to believe that any material that might have been stored in his computer in September 2002 would still be there at the time the ITO was drafted.

A) Possession of Electronic Material

[134] The appellant takes the position that "possession" implies that "an accused has made a decision to move the image beyond the public domain of the internet in order to harness child pornography in a place where the accused has control of the image". He draws a distinction between the offences of accessing and possession of child pornography and finds support for doing so in the reasons of the dissenting judge in the Court of Appeal, who found that there was no connection between the presence of the links in September 2002 and the probability of child pornography being present in the computer in January 2003.

[135] Three provisions of the *Criminal Code* are relevant to the discussion of the appellant's argument: the one defining possession and those establishing the offences of possession of and accessing child pornography. The provisions at the time of the search read as follows:

4. (3) For the purposes of this Act,

(a) a person has anything in possession when he has it in his personal possession or knowingly

(i) has it in the actual possession or custody of another person, or

(ii) has it in any place, whether or not that place belongs to or is occupied by him, for the use or benefit of himself or of another person; and

(b) where one of two or more persons, with the knowledge and consent of the rest, has anything in his custody or possession, it shall be deemed to be in the custody and possession of each and all of them.

[Possession of child pornography]

163.1...

(4) Every person who possesses any child pornography is guilty of(*a*) an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) an offence punishable on summary conviction.

[Accessing child pornography]

163.1...

(4.1) Every person who accesses any child pornography is guilty of

(*a*) an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) an offence punishable on summary conviction.

[Interpretation]

(4.2) For the purposes of subsection (4.1), a person accesses child pornography who

knowingly causes child pornography to be viewed by, or transmitted to, himself or

herself.

Although both s. 163.1(4) and s. 163.1(4.1) were amended in 2005, these amendments relate to the

duration of the sentence available and as such, do not impact the reasoning in this case.

[136] In the case at bar, it is not necessary to provide on exhaustive definition of the substantive offence of child pornography. Rather, this case may be decided on the narrower question — limited to the purpose of authorizing a search warrant — of what might be evidence of reasonable and probable grounds to believe that a person has committed the offence. However, even where the purpose is limited to this, it is essential to note that a specific intention to deal with the object in a particular manner is not an element of the offence of possession of child pornography. Sections 4(3)and 163.1(4) of the *Criminal Code* indicate that possession of child pornography is criminal in and of itself, irrespective of the use to which the accused intends to put the prohibited material. The appellant urges the Court to rely on R. v. York, 2005 BCCA 74, 193 C.C.C.(3d) 331, to import a further intent requirement. That case was also referred to with approval by the majority of the Court of Appeal. However, the intent requirement from York is inapposite to the offence of possession of child pornography as set out in the Criminal Code. The Crown need not demonstrate that an accused intended to "deal" with the pornographic material in a certain manner. The requisite mens rea will be established at trial if it is shown that the accused willingly took or maintained control of the object with full knowledge of its character. It is reasonable to conclude that in criminalizing simple possession, Parliament has assumed that an individual who possesses child pornography intends to use it in a "prohibited manner". This explains why statutory defences to charges relating to child pornography are provided in s. 163.1(6) of the Code — even if the elements of possession are made out, a person will not be convicted if he or she was in possession of child pornography for a "legitimate purpose" within the meaning of the Code and does not pose "an undue risk of harm" to someone under 18 years of age. The purpose for which an individual possesses child pornography does not change the fact of possession under the Code. What the defences mean is simply that in certain instances, criminal liability will not follow from a finding that the offence of possession of child pornography is made out on the facts. Not only is the Crown not required to prove at trial that the accused intended to deal with the material in a certain manner, but it is not necessary when applying for a search warrant to make out actual possession in the ITO. It is sufficient that there be credible evidence to support a reasonable belief that the search will uncover evidence of commission of the offence.

[137] A finding of actual possession within the meaning of s. 4(3)(*a*)(i) of the *Criminal Code* requires proof, among other things, that the person had physical control over the object, however brief that control may have been. As Doherty J.A. stated in *R. v. Chalk*, 2007 ONCA 815, 88 O.R. (3d) 448, at para. 19:

The Crown must also prove that an accused with the requisite knowledge had a measure of control over the item in issue. Control refers to power or authority over the item whether exercised or not: *R. v. Mohamad* (2004), 69 O.R. (3d) 481 (C.A.), at paras. 60-61.

See also *R. v. Terrence*, [1983] 1 S.C.R. 357; *R. v. Hess (No. 1)* (1948), 94 C.C.C. 48 (B.C.C.A.), approved in *Beaver v. The Queen*, [1957] S.C.R. 531.

[138] The same element must be found in the case of constructive possession (s. 4(3)(a)(i) *Criminal Code*): a person is in constructive possession if he or she has control — power or authority — however briefly, over an object located in a place (or space) — whether or not that place (or space) belongs to the person — for the use or benefit of the person or of a third person. Control is at issue in the case at bar.

[139] The appellant's submission with respect to what must be proven to establish possession thus goes beyond the legal definition of this element of the offence. In asserting that "the images must be present on the computer *itself* in order to be in [the] possession" of an accused, he defines control too narrowly (emphasis in original). As is clear from the wording of s. 4(3)(a)(ii) of the *Criminal Code* regarding constructive possession, the accused does not need to have control in a place belonging to him or her, such as his or her hard drive. The provision simply requires the material to be "in any place" for the use or benefit of the accused.

[140] This case does not require the Court to elaborate on the distinctions between accessing and possession of prohibited material. Suffice it to say that the question before us turns not on whether the accused has merely viewed the material, but on whether evidence of control over the material could be found in the computer that was to be searched. Accessing does not necessarily require control, and possession does not necessarily require viewing. Therefore, for the purposes of the offence of possession, viewing might be one way to prove knowledge of the content, but it is not the only way. Similarly, viewing might be one way to prove control, but it may not be sufficient — the circumstances in which the material was viewed would need to be proven. Control, not viewing, is the defining element of possession.

[141] Therefore, even if an accused does not actually download offending material, possession is established if the accused has control over the material for his or her use or benefit or for that of someone else. The record does not indicate that the reviewing judge was provided any evidence on caches. However, there is now abundant legal literature in which the authors have discussed caches, temporary Internet files, and deleted material that can be retrieved, all of which

may, under relevant circumstances, constitute evidence of possession. The degree of control might be established on the basis, for example, of the displaying of the images and the ability to select, cut, enlarge, print, forward or share images: see G. Marin, "Possession of Child Pornography: Should You Be Convicted When the Computer Cache Does the Saving for You?" (2008), 60 *Fla. L. Rev.* 1205, at p. 1212; T. E. Howard, "Don't Cache Out your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files" (2004), 19 *Berkeley Tech. L.J.* 1227; Akdeniz, at pp. 32-58 and 150-52; P. H. Luehr, "Real Evidence, Virtual Crimes: The Role of Computer Forensic Experts" (2005-2006), 20 *Crim. Just.* 14; R. Michaels, "Criminal Law — The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should Be Criminal" (2008), 30 *W. New Eng. L. Rev.* 817.

[142] In cases such as *R. v. Weir*, 2001 ABCA 181, 95 Alta. L.R. (3d) 225, *R. v. Daniels*, 2004 NLCA 73, 242 Nfld. & P.E.I.R. 290, and *Chalk*, Canadian courts of appeal have held that the Crown's burden is one of proving possession of prohibited material on the basis of control. Acts other than downloading complete files can be sufficient evidence of control for the purpose of obtaining a conviction for possession. When, as in *Weir*, the material is attached to an e-mail message, it may — even if the user has not downloaded it to his hard drive — serve as evidence of possession under relevant circumstances if, for example, the user either solicited the attachment or received it voluntarily with knowledge of its content. Similarly, when, as in *Daniels*, the computer user initiates the downloading of images but interrupts it, there is at least evidence of past control of the prohibited material. Distilled to their essence, these cases confirm that it is the assertion of control over the prohibited item that is at the core of the inquiry into whether possession was established, and that there is no requirement of a specific mode of control.

[143] When reviewing the authorization of a search for evidence of possession of child pornography, a court must therefore ask whether there was credible evidence to support a reasonable belief that an accused had control, and not, as the appellant contends, that the material had been downloaded and was in fact in the computer. With control as its focal point, possession must remain a flexible concept that will be applicable in the diverse contexts in which it will have to be applied as a result of technological change.

[144] The definition of possession advanced by the appellant and adopted by my colleague Fish J. could freeze possession in time and limit it to certain modes of storage and media. As a practical matter, there is little difference between exercising control over the hard drive of a computer while on the premises where the computer is located and exercising control over of the online space of a Web-based hosted service. Moreover, if, to bring a cache into the scope of possession, the accused were required to have knowledge of how caches work, this would require proof of intent or technical savvy on the part of the accused. As I mentioned above, the requisite mens rea will be established at trial if it is shown that the accused willingly took control of the object with full knowledge of its character. In light of the inevitability of technological change, it is important not to needlessly handcuff the courts to a concept of possession that is limited to certain technologies or to current-day computer practices. Control has been the defining feature of possession, not the possibility of finding data files on a hard drive. To adopt downloading as the threshold criterion would be to take a formalistic approach rather than drawing a principled distinction between access and possession. The classical approach to possession, rooted in control, therefore remains the most reliable one. It is the one that is most readily adapted to technological developments and it will not require courts to hear detailed forensic evidence of technological advances on an ongoing basis just to keep up with the times.

[145] The rules applicable to the authorization of a search do not change where the possession of electronic material is in issue. I would add that in view of the amount of material that can be found on the Internet, it is all the more important not to unduly restrict the concept of control: printing, enlarging and sharing are all actions which do not require downloading but may be evidence of control. Moreover, to limit possession to material downloaded to the computer of the accused would be to render constructive possession all but inapplicable in the context of the Internet. As I mentioned above, evidence of possession can take many forms and, although it must show control, is not limited to actual possession of the material.

[146] In the case at bar, the ITO appears to concern the likely discovery of both specified and unspecified types of evidence. Paragraph 15(c) of the ITO refers to a belief that the appellant would be in possession of "[i]mages that constitute child pornography", and para. 16 to searches for the purpose of finding images "or other evidence in regards to a charge under Section(s) 163.1(4) of the Criminal Code of Canada". The ITO could have been more precise with respect, for example, to evidence of control in caches or to the retrieval of deleted files. However, neither the reviewing judge's decision nor that of the Court of Appeal rested on evidence of control derived from caches or retrieved material, and the failure to be technologically specific is not determinative.

[147] Having concluded that what matters is evidence of possession based on control of the prohibited material, I cannot accept the appellant's argument that the issue is whether the presence of the two links labelled "Lolita Porn" and "Lolita XXX" in the "favourites" list of the Web browser's taskbar was sufficient to establish that the computer would contain downloaded images of child pornography. The issue is not whether downloaded images would be found, but whether evidence of possession would. Furthermore, all the circumstances must be considered, not just the presence of the two links. Bearing the real issue in mind, I will now turn to the appellant's arguments that the ITO was incomplete and that it contained false or boilerplate allegations, and to those concerning the probative value of the police officers' statements and the delay. I will conclude by discussing the reviewing judge's decision in light of the standards set in *Garofoli, Araujo* and *Pires*.

B) Omissions from the ITO and False and Boilerplate Allegations

[148] The rule enunciated in *Garofoli* and *Araujo* is that where an ITO contains erroneous or misleading information, the reviewing judge must expunge that information, which will no longer be admissible. In the present case, the appellant raised concerns about the drafting of the ITO to both the reviewing judge and the Court of Appeal.

[149] Before the reviewing judge, the appellant contended that the allegations relating to the child, the toys and the webcam were inflammatory and unnecessary. The judge found, on the contrary, that this information had to be included in the ITO to provide full and frank disclosure. It was required in order to explain the fact that Mr. Hounjet did not report his concerns to the police but consulted with his mother first, after which he informed the social worker, who in turn contacted the RCMP. This explained the delay in applying for the search warrant.

[150] The appellant formulated his argument in a slightly different way in the Court of Appeal, as he contended that the ITO contained boilerplate allegations, omissions, and erroneous statements. He submitted that the failure to mention that the child observed by Mr. Hounjet was his daughter and that the informant knew he resided with his wife could have misled the judge by creating an impression that the webcam and the toys were somehow linked to the offence of possession of child pornography, whereas there was no evidence supporting a conclusion that they were. The appellant also contended that the allegation that "the porn [was] removed" from the computer was false, since no child pornography was actually seen on the computer.

[151] As the reviewing judge indicated, the information concerning the presence of the child, the toys, and the webcam was necessary to convey to the authorizing judge Mr. Hounjet's concerns about the safety of the child. These facts prompted Mr. Hounjet to contact the social services office first instead of the police. This in turn explains part of the delay. From this perspective, the facts that the appellant was the child's father and that he resided with his wife were not determinative. In Mr. Hounjet's mind, what was at stake was the safety of *a* child. In addition, as I will explain below, the presence of the child, the toys, and the webcam form part of the entire set of relevant circumstances the authorizing judge could consider in deciding whether to issue the warrant.

[152] In this Court, the appellant adds that the second paragraph of the ITO is a boilerplate statement. This paragraph reads:

The Informant is presently involved in an investigation into the activities of Urbain

MORELLI, concerning violations of Section(s) 163.1(4) of the Criminal Code of Canada and in such capacity have access to and have reviewed the files and reports of other members of this police force who have been involved in this investigation and that the information received from them and referred to herein is based upon these files and reports and/or personal conversations with them.

[153] I cannot accept the appellant's argument. The paragraph serves as contextual support for the description of the investigation. It is preceded by a description of the informant's duties with the RCMP and by the statement that, except where otherwise mentioned, he has personal knowledge of the facts, and that he believes the facts of which he does not have personal knowledge to be true. In cross-examination, counsel for the appellant drew out the fact that the only police reports were those of the informant and of the other officer who was initially contacted by the social worker.

[154] Since the details of the investigation are set out in the paragraphs which follow the impugned statement, the authorizing judge could hardly read more into this introductory paragraph than what was said in the ITO. The reviewing judge and the majority of the Court of Appeal did not find that the allegations in the ITO were misleading and needed to be expunged. Even with this new argument added by the appellant in this Court, their findings should, in my view, be upheld. There is no indication that the allegations were meant to mislead or were so lacking in informational context that they should be excised from the ITO.

[155] Finally, the appellant argues that the references to the removal of child

pornography are false, because what was actually seen on the computer was not child pornography, but two links labelled "Lolita Porn" and "Lolita XXX". I do not agree with the appellant's characterization of the statements in the ITO. There could be no confusion about what was seen. In para. 5 of the ITO, "Lolita Porn" appears in quotation marks, and it is subsequently referred to in para. 10 as an "icon". The information set out in para. 10 is more detailed, as the informant gives a fuller account there of the statement made by Mr. Hounjet. There is no question that what had, according to Mr. Hounjet, been removed from the computer were the links in the "favourites" list to child pornography. Therefore the authorizing judge must have understood this to be the case.

[156] Hunter J.A., writing for the majority of the Court of Appeal, acknowledged that the drafting of the ITO was "less than perfect" (para. 51). But she found that the statements "do not breach the requirement of full and frank disclosure, nor trick the reader" (para. 58). I agree. Although the ITO could have been more elaborate in many respects, I agree with both the reviewing judge and the majority of the Court of Appeal that the omissions the appellant complains of do not support a conclusion that the ITO was so deficient that it did not provide the authorizing judge with a sufficiently credible factual basis.

C) Probative Value of the Police Officers' Statements

[157] In paragraph 12 of the ITO, the informant indicated that he had spoken with Cpl. Boyce, who had stated that "these type[s] of offenders are habitual and will continue their computer practices with child pornography". Cpl. Boyce had added that "this information will remain inside the harddrive of the computer and can be stored on media devices such as compact disks and floppy disks". In paragraph 13, the informant related a conversation with Cst. Huisman, who had stated that "offenders treasure collections on their computer and like to store them and create backup's (*sic*) in case they loose it (*sic*)".

[158] The appellant contends that these officers were not qualified to provide opinion evidence on child pornography and that there was no basis for concluding that he was a habitual child pornography offender.

[159] More contextual information on both the subject matter of the officers' statements and their source would have made it easier to understand and assess them. However, there is no indication that the officers were not qualified or that there was any intention to mislead. Consequently, it was open to the reviewing judge to receive evidence which amplified the information and conclude that the authorizing judge was provided with sufficient evidence.

[160] The ITO indicated that Cpl. Boyce was with the RCMP's Technological Crime Unit in Regina and that Cst. Huisman was with the Saskatoon Police Service's Vice Unit. The reviewing judge learned from the examination of the informant, Cst. Ochitwa, that he had had advance knowledge of Cpl. Boyce's expertise in computer technology. Indeed, Cpl. Kusch of the RCMP, who was originally in charge of the investigation, had also contacted Cpl. Boyce with regard to the links and their relationship to child pornography. As for Cst. Huisman, the informant had contacted him at the suggestion of a Crown prosecutor in Regina. Cst. Ochitwa understood Cst. Huisman to be an expert in child pornography as a result of conversations he had had both with the Crown prosecutor and with Cst. Huisman himself. [161] Obtaining clarifications that might demonstrate that the officers were not qualified to provide the information they did was within the purview of the *voir dire*. Defence counsel cross-examined the informant in the course of that proceeding and did little to undermine the credibility of the evidence. The only fact that was added as a result of the cross-examination was that the informant did not know how long the officers had been working in their units. If defence counsel thought they were not qualified, he could have examined them individually. This, however, would have entailed risks counsel may not have wanted to take. An appeal should not be a forum for belatedly correcting strategic decisions that did not turn out as counsel would have hoped.

[162] It was neither inappropriate nor erroneous to rely on the information provided by Cpl. Boyce and Cst. Huisman about the propensity of child pornography offenders to collect and hoard such materials. Indeed, this propensity, which seems to be notorious, has been accepted in numerous child pornography cases as part of the factual backdrop giving rise to reasonable and probable grounds for issuing search warrants, and it has also been noted in the academic commentary on child pornography: *R. v. Neveu*, 2005 NSPC 51, 239 N.S.R. (2d) 59, at paras. 15-17; *R. v. Fawthrop* (2002), O.A.C. 350, at para. 14; *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006), at pp. 1068 and 1072; *United States v. Martin*, 426 F.3d 68 (2nd Cir. 2006), at pp. 72 and 75; *United States v. Shields*, 458 F.3d 269 (3rd Cir. 2006), at p. 279; *Davidson v. United States*, 213 Fed.Appx. 769 (11th Cir. 2006), at p. 771; *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008); *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008), at p. 1206; M. Taylor and E. Quayle, *Child Pornography: An Internet Crime* (2003), chapter 7 "The Process of Collecting". Even if a lay person would not necessarily know that child pornography offenders collect such material, this appears to be

something law enforcement officials working in computer technology or vice units encounter frequently. Testimony about this fact cannot therefore be compared to testimony about novel technology or science: *R. v. Mohan*, [1994] 2 S.C.R. 9; *R. v. J.-L.J.*, 2000 SCC 51, [2000] 2 S.C.R. 600; *R. v. Trochym*, 2007 SCC 6, [2007] 1 S.C.R. 239.

[163] I would not dismiss the impugned statements on the basis that, because the proof of the officers' expertise was insufficient, their statements have no probative value. Providing the judge with the officers' credentials could have enhanced or reduced the probative value of their statements. However, the positions the officers held in their respective forces was sufficient to support a conclusion that their statements had sufficient probative value to be included in the ITO.

[164] As for the appellant's second argument, that there was no basis for the officers to say that he was a habitual child pornography offender, it can be disposed of by pointing out that it is not what the officers stated. The conversations between the informant and the other officers took place several months after Mr. Hounjet's visits, and they related to what material might be found in the computer and whether material would still be found there despite the time elapsed between the visits and the swearing of the ITO. These are facts that the informant had to put before the authorizing judge.

[165] In the body of the ITO, the officers' statements were placed after the description of the facts giving rise to the grounds to believe that evidence of the commission of the offence would have been found at the time of Mr. Hounjet's visits. I agree with the appellant that the statements could not be used to characterize him as a type of person who is likely to be a child pornography offender. Indeed, the officers were never asked to make such a statement about the appellant, and they offered no opinion on this point.

[166] It was for the reviewing judge to decide whether the allegations put before the authorizing judge, as amplified, could provide a credible basis for concluding that evidence of the possession of child pornography would likely be found in the computer. Hunter J.A. agreed with the reviewing judge that they could. As I explain in greater detail below, I also agree, having regard to all the facts, that there was a basis for the reviewing judge to draw the necessary inferences.

[167] The appellant also contends that the meaning of the expression "type of offenders" needs to be explained to be understood. I cannot accept this argument. Although police officers should draft ITOs as precisely and clearly as possible, reviewing judges must attempt to make sense of the material that is presented to them and request details or additional information if they feel an ITO is not clear on an important element. The reviewing judge in this case concluded, rightly in my view, that the allegations made sense.

D) Delay Elapsed Between Mr. Hounjet's Visits and the Swearing of the ITO

[168] The appellant submits that in view of the four-month delay after Mr. Hounjet had noticed the links on his computer, it was not reasonable to conclude that he still had the computer in question in his residence and that any "child pornography" was still in the house when the ITO was sworn.
[169] The issue of the delay was raised — unsuccessfully — both before the reviewing judge and in the Court of Appeal. The reviewing judge was satisfied that the inquiry made at SaskTel on January 8, 2003 to determine whether the appellant had an active Internet connection disposed of any question about whether the appellant still had his computer. She found:

It logically follows that the subscription could only be utilized with a computer. The Justice of the Peace could have been satisfied that there was a basis for Cst. Ochitwa to believe the accused's computer was in the premises that were the subject of the search warrant. [para. 21]

[170] In assessing the appellant's argument on delay, the Court of Appeal also referred to the statements in the ITO about how material is stored in a computer. Hunter J.A., for the majority, concluded:

Therefore, on reading the whole of the Information, the delay was disclosed. There was adequate information about the storage of materials on a computer, together with evidence confirming the current residence of the appellant and a continuing Internet connection, for the justice of the peace to have reasonable grounds to believe that the item(s) sought was in the computer in the appellant's residence. [para. 50]

[171] This conclusion should, in my view, be upheld. The appellant's contention that it was not reasonable for the judge to conclude that the computer would still be in the residence four months after Mr. Hounjet's visits is not valid. Unlike in the case of food or other goods with a short useful lifespan, there was no reason to presume that the appellant would have changed his computer

within four months after the visits. In addition, there was no indication that the computer was in any way in need of being replaced. It was therefore appropriate for the informant to rely on common sense and on the ongoing subscription to an Internet connection to support his allegation that the computer was still in the appellant's residence. A further issue was whether there would still be evidence of the possession of child pornography in the computer. Even if it had been doubtful that the *same* computer was still in the residence, the police officers' statements concerning the proclivity of child pornography users to save and collect such material would have alleviated most concerns about the likelihood of finding evidence of possession of child pornography.

[172] I have already discussed the admissibility of the statements of Cpl. Boyce and Cst. Huisman. It was on the issue of the delay that they became relevant. As stated in the ITO, Cpl. Boyce said that "these type of offenders are habitual and will continue their computer practices with child pornography". He added that "this information will remain inside the hardrive of the computer and can be stored on media devices". These statements could serve as a basis for concluding that it was reasonable to believe that, if the appellant was this type of offender, evidence of the offence would still be found in the computer after four months. The evidence in question would relate to the appellant's computer practices and would continue to be stored in the computer or on media devices. Cst. Huisman's statement, found in the ITO, that "offenders treasure collections on their computer and like to store them and create backup's (*sic*) in case they loose it (*sic*)" is also relevant to the delay.

[173] In child pornography cases, Canadian and American courts have frequently upheld warrants issued months and even years after the occurrence of the facts relied upon for the search. In their decisions, they have relied on various combinations of three elements: the proclivity of offenders to collect child pornography, the application of common sense in light of the nature of the material, and the ability of computer forensics examiners to recover data. For example, in *Neveu* more than four years had elapsed between the closing of a website on which paying subscribers accessed child pornography and the issuance of the warrants. In *Neveu*, the judge explained his rejection of a staleness argument as follows:

Child pornographic images on the other hand, as disclosed in the Information to Obtain, are likely held for much longer periods of time by individuals who purchase them than the items mentioned above. In addition to relying on the opinion to that effect set out in the Information to Obtain herein, the issuing Justice could have also concluded, employing her common sense, that the retention of child pornographic images is likely more analogous to the lawful acquisition and collection of books, C.D.'s, D.V.D.'s, photographs, paintings and such items which offer the prospect of ongoing enjoyment thereby giving them their collectable nature. Collectible items are distinctively different than items which are consumable or acquired for quick resale. [para. 15]

Similarly in *R. v. Graham*, 2007 Carswell PEI 80 (Prov. Ct.), at paras. 27-32, aff'd 2008 PESCAD 7, 277 Nfld & P.E.I.R. 103, the warrant was initially issued four years after the alleged downloading (although in that case the warrant was quashed on review on other grounds). Examples also abound in the United States: *Gourde* (four months); *Shields*, at p. 279 (nine months); *Perrine* (111 days); *United States v. Terry*, 522 F.3d 645 (6th Cir. 2008) (five months).

[174] If the offence of possession of child pornography is approached as one that requires evidence of past or present control of the prohibited material and does not require evidence that the prohibited material has been downloaded or permanently saved, little needs to be added on the issue of delay. What does require examination is the constellation of facts that could serve as a basis for the judge to characterize the appellant as a "type of offender" who is likely to collect prohibited material. I will turn to this question now.

E) Sufficiency of the Grounds for Issuing the Warrant

[175] It is important to mention the standard of review: the reviewing judge does not substitute his or her opinion on the sufficiency of the grounds for authorizing the search for that of the authorizing judge. I reiterate Charron J.'s comment in *Pires* (at para. 30) that in a *Garofoli* hearing, the basis for exclusion is relatively narrow. The reviewing judge "only inquires into whether there was any basis upon which the authorizing judge could be satisfied that the relevant statutory preconditions existed" (para. 30).

[176] As I mentioned above in para. 130, the reviewing judge determines whether there was credible evidence on which the issuing judge's decision could be based. To conduct this inquiry, the judge can look not only at the ITO but also at the evidence as amplified at the review hearing.

[177] In the case at bar, the appellant focuses on the presence of two links in the "favourites" list of his Web browser's taskbar. However, the overall circumstances go beyond the

mere presence of those two links. They can be briefly outlined as follows:

1. *Surprise*: The appellant appeared surprised when Mr. Hounjet arrived at his residence. In itself, this fact could be seen as neutral. However, the sequence of events that followed Mr. Hounjet's arrival shaped the information and gave it significance.

2. *Interest in both adult and child pornography*: While Mr. Hounjet worked on the computer, he noticed links to adult and child pornography in the "favourites" list of the Web browser's taskbar. He also noticed a pornographic image, but he could not remember afterwards if it was on the browser's home page or on the computer desktop. The image was so "graphic" that he wondered if the appellant's wife "let him view and keep it on as their desktop".

3. *Conspicuous interest in pornography*: The presence of adult pornography does not in itself support a finding that the alleged offence was committed. However, when either the desktop or the Web browser's home page has been customized by adding an image, the image becomes unavoidable and can be evidence that the user has a conspicuous interest in pornography. This conclusion is reinforced by the presence of the links to adult pornography in the "favourites" list.

4. *Pronounced interest in child pornography*: The fact that there was more than one link to child pornography supported an inference that the appellant's interest in child pornography was pronounced.

5. *Deliberate acts*: The facts that the links to adult and child pornography were placed in the "favourites" list and that there was a pornographic image either on the home page or on the desktop were evidence that the computer user had placed them there deliberately.

6. *Intention to facilitate access*: The fact that the impugned links were in the "favourites" list of the Web browser's taskbar supported inferences that the sites to which they led were ones the user intended to access easily and that they may have been placed there for regular use.

7. Use of multiple devices to record images: The presence of a webcam connected to a videotape recorder and of videotapes, both labelled and unlabelled, supported an inference that the computer user was in the habit of recording images on videotapes or other devices, that the practice was current, and that the user had multiple devices on which images could be stored so that he could view them at will.

8. *Current practice of recording images*: The fact that the camera was pointed at the child and the toys while it was connected to the videotape recorder indicated that the practice of recording images was current.

9. Acts to avoid arousing suspicion: The fact that upon Mr. Hounjet's return the next day, the camera had been turned toward the computer user's seat supported an inference that the appellant had deliberately moved it to avoid arousing suspicion occasioned by the fact that it was initially pointed at the child's play area.

10. Acts to prevent the technician from seeing the links to pornography and the *image*: The fact that at the time of the second visit, the computer had been formatted and all the links to pornography, including in particular the two links to child pornography, as well as the image seen either on the home page or on the desktop had been removed supported an inference that the appellant wanted to prevent the technician from seeing the links and the image, or from accessing some other similar content.

11. Connection between the "tidying up" and the removal of the pornographic *material*: The fact that the videotapes had been put away before the second visit indicated that the appellant was not indifferent to them being in plain sight. Viewed in isolation, the tidying up of the room might be seen as insignificant, but the fact that it coincided with the "tidying up" of the computer supports an inference of a connection between the removal of the pornographic items from the computer and the appellant's desire to prevent an observer from noting that he was in the habit of recording and saving images.

[178] The reviewing judge's task is not to determine whether in his view the evidence is sufficient to support a finding that the accused is guilty of the alleged offence. The relevant question is simply whether there was a credible basis for issuing the warrant. In other words, in the instant case, the question is whether the facts alleged in the ITO as amplified at the *voir dire* were sufficient for the reviewing judge to conclude that there was a basis for the authorizing judge's decision. Since the ITO submitted to the authorizing judge referred to both direct and circumstantial evidence, it is worth recalling the comments

of McLachlin C.J. in *R. v. Arcuri*, 2001 SCC 54, [2001] 2 S.C.R. 828, at para. 23, concerning the task a judge must perform in assessing the sufficiency of circumstantial evidence. Although these comments were made in the context of a preliminary enquiry, they are relevant to the decision of a judge reviewing the authorization of a search where circumstantial evidence has been presented:

The judge's task is somewhat more complicated where the Crown has not presented direct evidence as to every element of the offence. The question then becomes whether the remaining elements of the offence — that is, those elements as to which the Crown has not advanced direct evidence - may reasonably be inferred from the circumstantial evidence. Answering this question inevitably requires the judge to engage in a limited weighing of the evidence because, with circumstantial evidence, there is, by definition, an inferential gap between the evidence and the matter to be established — that is, an inferential gap beyond the question of whether the evidence should be believed: see Watt's Manual of Criminal Evidence, supra, at §9.01 (circumstantial evidence is "any item of evidence, testimonial or real, other than the testimony of an eyewitness to a material fact. It is any fact from the existence of which the trier of fact may infer the existence of a fact in issue"); *McCormick on Evidence, supra*, at pp. 641-42 ("[c]ircumstantial evidence... may be testimonial, but even if the circumstances depicted are accepted as true, additional reasoning is required to reach the desired conclusion"). The judge must therefore weigh the evidence, in the sense of assessing whether it is

<u>reasonably capable of supporting the inferences that the Crown asks the jury to</u> <u>draw.</u> This weighing, however, is limited. The judge does not ask whether she herself would conclude that the accused is guilty. Nor does the judge draw factual inferences or assess credibility. The judge asks only whether the evidence, *if believed*, <u>could reasonably support an inference</u> of guilt. [Italics in original; underlining added.]

[179] In this case, the authorizing judge had direct evidence of some facts but many others required inferences. In addition, the evidence was amplified before the reviewing judge. The appellant's surprise when Mr. Hounjet arrived unannounced could reasonably support an inference that he was uncomfortable giving the technician access to the computer while sensitive material could be found there. The reviewing judge was told: "The icons themselves that would appear on the desktop are added by the user themself" (A.R., at p. 134). Therefore, the facts that there were several links to both adult and child pornography in the "favourites" list and that a "graphic" pornographic image was prominently displayed on the computer justified the judge's drawing the reasonable inference that the appellant had a conspicuous interest in this type of material. His specific interest in child pornography was shown by the deliberate addition to his "favourites" list of links to child pornography. The fact that there were two links indicated that this interest was pronounced. Their presence in the "favourites" list also indicated that the appellant wanted to have easy access to the websites. The position of the camera and the fact that it was connected to a videotape recorder at the time of the technician's first visit, together with the presence of both labelled and unlabelled videotapes, showed that he was interested in

reproducing images, accumulating such material, and keeping it for his future use. The appellant's desire not to arouse suspicion with respect to his reproduction of images or his computer practices could reasonably be inferred from his actions after being informed that the technician needed to return: removing the videotapes from the room, changing the direction the camera was pointed in, reformatting the computer and, more particularly, removing the suspect image and links. These actions by the appellant were relatively unexceptional if considered individually and out of context, but if viewed globally, it was possible for them to lead the reviewing judge to conclude that the authorizing judge had not erred in issuing the warrant. There was a credibly based probability that the appellant was in the habit of reproducing and saving images and had a propensity to pornography, and more specifically to child pornography.

[180] Once it is accepted that the judge could infer that the appellant propended towards child pornography, it must also be accepted that he could conclude that, in view of the appellant's habit of reproducing and saving images, there were reasonable grounds to believe that at the time of Mr. Hounjet's visits, the appellant was in possession of child pornography. This conclusion is all the more reasonable in light of the fact that evidence of sufficient control to establish possession can take many forms and can relate to past or present possession.

[181] The police officers' statements could not be used to demonstrate that the appellant was a type of person who was likely to be in possession of child pornography, but given that there is credible independent evidence of this, they do shed light on the

implications of that evidence. In these circumstances, the statements that child pornography offenders are collectors could only make it more likely that evidence of the possession of prohibited material would still exist at the time Cst. Ochitwa drafted the ITO.

III. Conclusion

[182] A review by an appellate court of the sufficiency of the initial grounds for issuing a search warrant remains a delicate exercise. This is why the grounds for reviewing the authorizing judge's decision are so narrow. It is also why deference is owed to the decision of the reviewing judge, who sees and hears the witnesses. In the case at bar, to echo LeBel J.'s words in *Araujo*, I conclude that "there was reliable evidence that might reasonably be believed on the basis of which the authorization could have issued" (para. 54 (emphasis deleted)). Therefore, the reviewing judge and the majority of the Court of Appeal did not make reversible errors in upholding the authorizing judge's decision.

[183] Since I conclude that the search warrant was validly issued, I do not need to consider the issue of exclusion of the evidence. For these reasons, I would dismiss the appeal.

APPENDIX

The Information to Obtain the Search Warrant is as follows:

•••

The Informant says that Urbain MORELLI of 520 Gibson Street, La Ronge, Saskatchewan is in possession of obscene material which depicts, advocates, or counsels sexual activity with a person under 18 years of age, contrary to Section 163.1(4) of the Criminal Code of Canada, and whereas it appears that a computer, brand name and serial number unknown, the property of Urbain MORELLI, and that the Informant has reasonable grounds for believing that the said material, or some part of them are contained inside the computer, the property of Urbain MORELLI, that is presently in the dwelling house and/or outbuildings, and/or vehicles registered to the address of 520 Gibson Street, La Ronge, Saskatchewan and that

- 1. The Informant is a member of the Royal Canadian Mounted Police, presently assigned to the General Investigation Section of the La Ronge Detachment and has personal knowledge of the facts and matters herein deposed to except where stated to be otherwise and where so stated do verily believe the same to be true.
- 2. The Informant is presently involved in an investigation into the activities of Urbain MORELLI, concerning violations of Section(s) 163.1(4) of the Criminal Code of Canada and in such capacity have access to and have reviewed the files and reports of other members of this police force who have been involved in this investigation and that the information received from them and referred to herein is based upon these files and reports and/or personal conversations with them.
- 3. For the purposes of this information, a "computer" is a box that houses a central processing unit (hereinafter referred to as a CPU) along with other internal storage devices (such as internal hard drives) that store information in the form of files. A "computer" also contains internal communication devices (such as internal modems capable of sending and receiving electronic mail or fax) along with any other hardware stored or housed internally. Thus, a "computer" for the purpose of this information refers to hardware, software, and data contained in the main unit, printers, external modems (attached by a cable to the main unit), monitors and any other external attachments will be referred to collectively as peripherals. When the computer and all peripherals are referred to as one package, the term "computer system" is used.
- 4. The Informant believes that Urbain MORELLI may be in possession of material supporting the charge of possession of Child Pornography, contrary to Section 163.1(4) of the Criminal Code of Canada. The Informant also believes that there is presently a computer, the property of Urbain MORELLI, at the above noted premises.
- 5. During the first week of August, 2002, Adrien HOUNJET, a technician for the Keewatin Career Development Corporation, attended a residence in La Ronge on Gibson Street to install SaskTel high speed Internet on a computer. Once on the computer HOUNJET observed "Lolita Porn" on the screen and a web-cam pointing

towards toys. The client was alone in the house with a three year old child. HOUNJET was unable to complete the work and returned the next day to find the porn removed and the toys cleaned.

- 6. Adrien HOUNJET later consulted with his mother and decided to contact Social Services to report his observations.
- 7. On November 15, 2002, Adrien HOUNJET attended to the Social Services office in La Ronge and completed a report with Lillian SANDERSON, a Social Services employee, outlining what he discovered during the installation.
- 8. On November 18, 2002, Val FOSSENEUVE, of La Ronge Social Services, called the La Ronge Detachment for assistance in investigating this report. FOSSENEUVE reported HOUNJET's findings to Corporal Susan KUSCH.
- 9. With information received from FOSSENEUVE, Corporal KUSCH called Corporal Mike BOYCE, of the Royal Canadian Mounted Police, Technological Crime Unit in Regina, Saskatchewan. Corporal Mike BOYCE confirmed that "Lolita" is an underage internet porn site that primarily deals with children 14 years old and under.
- 10. On January 8, 2003 the Informant obtained a detailed statement from Adrien HOUNJET. HOUNJET stated at the end of July, or early August he entered a yellow trailer on Gibson Street to install SaskTel high speed internet. Upon entering the room where the computer was located, HOUNJET observed a web-cam aimed at childrens (*sic*) toys on the floor. The web-cam was hooked up to a black VCR where several blank videotapes were found. Once on the computer, HOUNJET discovered child pornography icons on the desktop and a pornographic home-page. Some of the icons included "Lolita Porn" and "Lolita XXX". HOUNJET was unable to complete the installation so made arrangements to come back the following morning. When he arrived the next day, the childrens (*sic*) toys were cleaned up, the videotapes were gone and the web-cam was pointed to the computer chair. HOUNJET noted all the child porn off the computer was gone and the hardrive was formatted.
- 11. On January 8, 2003 the Informant personally drove on Gibson Street in La Ronge and confirmed the only yellow trailer is the residence of 520 Gibson Street. Parked in the driveway of this residence was a grey Ford Aerostar, bearing Saskatchewan licence 594 AJD. A police inquiry on this licence revealed this vehicle is registered to Urbain MORELLI.
- 12. On January 9, 2003 the Informant personally spoke with Corporal Mike BOYCE. Corporal BOYCE states these type of offenders are habitual and will continue their computer practices with child pornography. Corporal BOYCE stated this Information will remain inside the hardrive of the computer and can be stored on media devices such as compact disks and floppy disks.

- 13. On January 9, 2003 the Informant also spoke with Constable Randy HUISMAN of the Saskatoon Police Service, Vice Unit in Saskatoon, Saskatchewan. Constable HUISMAN stated offenders treasure collections on their computer and like to store them and create backup's (*sic*) in case they loose it (*sic*). Discs and floppy disks are used for this purpose. Offenders will typically sort information and store pictures on different file names to catagorize (*sic*) them.
- 14. On January 9, 2003 Adrien HOUNJET called the Informant to report he reviewed his work order and initially attended to Urbain MORELLI's residence at 520 Gibson Street on September 5, 2002 at 2:20pm for the high speed installation.
- 15. As a result of the investigation that was described in the above paragraphs, it is believed that Urbain MORELLI is in possession of the following:
 - a) Electronic devices which are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data. These devices include computer, computer components, computer peripherals, word processing equipment, encryption secret boards, internal had (*sic*) drives and modems.
 - b) Any instructions and programs stored in the form of electronic or magnetic media, which are capable of being interpreted by a computer or related components. These items to be seized include applications software, utility programs, compilers, interpreters, and any other programs or software used to communicate with computer hardward (*sic*) or peripherals either directly or indirectly via telephone lines, radios or any other means of transmission.
 - c) Images that constitute child pornography.
- 16. By searching for and seizing the above described computers, searches can be conducted on those same computer's internal files and directories for images described above or other evidence in regards to a charge under Section(s) 163.1(4) of the Criminal Code of Canada.

. . .

Appeal allowed, DESCHAMPS, CHARRON and ROTHSTEIN JJ. dissenting.

Solicitors for the appellant: McDougall Gauley, Regina.

Solicitor for the respondent: Attorney General for Saskatchewan, Regina.