Her Majesty the Queen v. Jones
[Indexed as: R. v. Jones]

107 O.R. (3d) 241
2011 ONCA 632
Court of Appeal for Ontario,
MacPherson, Blair and Epstein JJ.A.
October 11, 2011

Charter of Rights and Freedoms -- Exclusion of evidence -- Search and seizure -- Police obtaining warrant to search accused's computer for evidence of fraud -- Police analyst finding initial images of child pornography while seeking evidence of fraud -- Police seeking advice from Crown who erroneously advised police that they did not have to obtain another warrant -- Police then searching types of files would not have examined for fraud investigation to determine if accused having more child pornography -- Subsequent search violating accused's rights under s. 8 of *Charter* -- Crown acting in good faith in unsettled area of law and trial judge erring by finding incorrect advise demonstrating systemic failure -- Police acting in good faith -- Somewhat serious but not at end of spectrum of serious breaches as trial judge found -- Violation having significant impact on accused -- Child pornography videos found in course of subsequent search being reliable evidence of abhorrent crime and being important to Crown's case very high societal interest in having case tried on merits -- Admission of evidence of videos not bringing administration of justice into disrepute -- *Canadian Charter of Rights and Freedoms*, ss. 8, 24(2).

Charter of Rights and Freedoms -- Search and seizure -- Police obtaining warrant to search accused's computer for evidence of fraud -- Warrant authorizing unlimited access to computer's files in order to accomplish objective of search -- Police analyst finding images of child pornography while searching for evidence of fraud -- Police seeking Crown's advice about whether further warrant required before searched types of files would not have examined during fraud investigation -- Crown erroneously advising police that initial search warrant sufficient -- Analyst then looking at video files solely for purpose of searching for child pornography -- Search of video files for child pornography not authorized by initial warrant -- Plain view doctrine justifying search and seizure of images found during first review of files but not justifying subsequent search of video files -- Subsequent search not authorized under s. 489 of *Criminal Code* -- Subsequent search violating accused's rights under s. 8 of *Charter* -- *Canadian Charter of Rights and Freedoms*, s. 8 -- *Criminal Code*, R.S.C. 1985, c. C-46, s. 489.

The accused was charged with possession of child pornography. The police obtained a warrant to search the accused's computer for evidence of fraud. The warrant contained no restrictions on the types of files that could be searched, nor was it limited by date of the file. During his initial review of the document and image files, the police analyst found images that he believed constituted child pornography. He asked the investigating officer to contact the Crown to determine whether a warrant should be obtained to search for child pornography. The Crown advised the police that no further warrant was required. A second officer then spoke with the Crown to ensure that he understood that the search for child pornography would entail types of files that wouldn't have been examined as part of the search related to the fraud. The Crown reiterated his opinion that no additional warrant was required. During a subsequent search, the analyst searched the video files and found more child pornography. The trial

judge found that the accused's rights under s. 8 of the *Canadian Charter of Rights and Freedoms* were violated as the warrant did not authorize a review of the computer hard drive for anything other than evidence of fraud. She classified the advice given to the police as "reckless and cavalier" and symbolic of an institutional failure. She excluded the child pornography evidence under s. 24(2) of the *Charter*. The accused was acquitted. The Crown appealed.

Held, the appeal should be allowed.

The search warrant did not authorize a search for evidence of child pornography. While it contained no limitations on the types of files that could be examined, it was limited in the types of evidence the police could seek, and that evidence did not include evidence of child pornography. The right to examine the entire contents of a computer for evidence of one crime does not carry with it the untrammelled right to rummage through the entire computer contents in search of evidence of another crime. A computer search pursuant to a warrant must be related to the legitimate targets respecting which the police have reasonable and probable grounds, as articulated in the warrant. The Crown was correct that the child pornography in image files that was unexpectedly observed as part of the search for evidence of the fraud covered by the search warrant was authorized by the plain view doctrine and under s. 489 of the *Criminal Code*. However, the same could not be said for the images found in video files in the course of the subsequent search that was specifically seeking evidence of images of child pornography. The Crown's argument was once a computer is lawfully seized, one loses all expectations of privacy; one loses only the expectation of privacy with respect to those portions of the computer that the police are lawfully entitled to search. The accused's rights under s. 8 of the *Charter* were violated by the search of video files aimed at investigating whether there were additional images of child pornography.

The trial judge erred in characterizing the Crown's conduct as "cavalier or reckless". There was no appellate authority at the time governing the application of the plain view doctrine or of s. 489 of the Code in the computer search context. While the Crown's advice turned out to be wrong, the Crown acted in good faith, the law was unsettled at the time as to application of the plain view doctrine and as to the scope of s. 489 in the context of computer searches. Moreover, there was no evidence of a systemic failure in the Crown's office. The police also acted in good faith as evidenced by seeking legal guidance before searching the video files. The breach of the accused's *Charter* rights was somewhat serious, but was not at the most serious end of the spectrum. As the accused had a high expectation of privacy in the contents of his computer, the violation had a significant impact on his *Charter*-protected rights. The evidence in question was reliable and was important, but not crucial, to the Crown's case. The offence was very serious. On balance, exclusion of the evidence would bring the administration of justice into disrepute.

APPEAL by the Crown from an acquittal entered by Nolan J. of the Superior Court of Justice on a charge of possession of child pornography on July 2, 2010.

Cases referred to *R. v. Grant*, [2009] 2 S.C.R. 353, [2009] S.C.J. No. 32, 2009 SCC 32, 82 M.V.R. (5th) 1, 309 D.L.R. (4th) 1, 245 C.C.C. (3d) 1, EYB 2009-161617, J.E. 2009-1379, 66 C.R. (6th) 1, 193 C.R.R. (2d) 1, 391 N.R. 1, 253 O.A.C. 124; *R. v. Morelli*, [2010] 1 S.C.R. 253, [2010] S.C.J. No. 8, 2010 SCC 8, 207 C.R.R. (2d) 153, 399 N.R. 200, EYB 2010-171050, 2010EXP-1068, J.E. 2010-576, 252 C.C.C. (3d) 273, 316 D.L.R. (4th) 1, [2010] 4 W.W.R. 193, 72 C.R. (6th) 208, 346 Sask. R. 1, 86 W.C.B. (2d) 949, apld

R. v. Lefave, [2003] O.J. No. 3861, [2003] O.T.C. 872, 59 W.C.B. (2d) 217 (S.C.J.); *R. v. Weir*, [2001] A.J. No. 869, 2001 ABCA 181, [2001] 11 W.W.R. 85, 95 Alta. L.R. (3d) 225, 281 A.R. 333, 156 C.C.C. (3d) 188, 85 C.R.R. (2d) 369, 50 W.C.B. (2d) 463; *United States of America v. Comprehensive Drug Testing Inc*., 579 F.3d 989 (9th Cir. 2009), revised 621 F.3d 1162 (9th Cir. 2010); *United States of America v. Williams*, 592 F.3d 511 (4th Cir. 2010), cert. denied *Williams v. United States of America*, 131 S. Ct. 595, 178 L. Ed. 2d 434 (2010), consd

Other cases referred to *Hunter v. Southam Inc.*, 1984 CanLII 33 (SCC), [1984] 2 S.C.R. 145, [1984] S.C.J. No. 36, 11 D.L.R. (4th) 641, 55 N.R. 241, [1984] 6 W.W.R. 577, J.E. 84-770, 33 Alta. L.R. (2d) 193, 55 A.R. 291, 27 B.L.R. 297, 14 C.C.C. (3d) 97, 2 C.P.R. (3d) 1, 41 C.R. (3d) 97, 9 C.R.R. 355, 84 D.T.C. 6467; *R. v. Arp*, 1998 CanLII 769 (SCC), [1998] 3 S.C.R. 339, [1998] S.C.J. No. 82, 166 D.L.R. (4th) 296, 232 N.R. 317, [1999] 5 W.W.R. 545, J.E. 98-2397, 114 B.C.A.C. 1, 58 B.C.L.R. (3d) 18, 129 C.C.C. (3d) 321, 20 C.R. (5th) 1, 40 W.C.B. (2d) 196; R. v. B. (E.), [2011] O.J. No. 1042, 2011 ONCA 194, 276 O.A.C. 173, 269 C.C.C. (3d) 227, 94 W.C.B. (2d) 386; *R. v. Bishop*, [2007] O.J. No. 3806, 2007 ONCJ 441, 75 W.C.B. (2d) 258; *R. v. Collins*, 1987 CanLII 84 (SCC), [1987] 1 S.C.R. 265, [1987] S.C.J. No. 15, 38 D.L.R. (4th) 508, 74 N.R. 276, [1987] 3 W.W.R. 699, J.E. 87-516, 13 B.C.L.R. (2d) 1, 33 C.C.C. (3d) 1, 56 C.R. (3d) 193, 28 C.R.R. 122, 15 W.C.B. (2d) 387; *R. v. DeJesus*, [2010] O.J. No. 3744, 2010 ONCA 581; *R. v. Dore*, 2002 CanLII 45006 (ON CA), [2002] O.J. No. 2845, 162 O.A.C. 56, 166 C.C.C. (3d) 225, 4 C.R. (6th) 81, 96 C.R.R. (2d) 49, 54 W.C.B. (2d) 691 (C.A.); *R. v. Du*, [2004] A.J. No. 1324, 2004 ABQB 849, 65 W.C.B. (2d) 720; *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82, 55 D.L.R. (4th) 503, 89 N.R. 249, J.E. 89-77, 73 Nfld. & P.E.I.R. 13, 45 C.C.C. (3d) 244, 66 C.R. (3d) 348, 38 C.R.R. 301, 10 M.V.R. (2d) 1, 6 W.C.B. (2d) 78; *R. v. Edwards* (1996), 1996 CanLII 255 (SCC), 26 O.R. (3d) 736, [1996] 1 S.C.R. 128, [1996] S.C.J. No. 11, 132 D.L.R. (4th) 31, 192 N.R. 81, J.E. 96-349, 88 O.A.C. 321, 104 C.C.C. (3d) 136, 45 C.R. (4th) 307, 33 C.R.R. (2d) 226, 29 W.C.B. (2d) 366; *R. v. F. (L.)*, 2002 CanLII 45004 (ON CA), [2002] O.J. No. 2604, 161 O.A.C. 350, 166 C.C.C. (3d) 97, 96 C.R.R. (2d) 20, 54 W.C.B. (2d) 652 (C.A.); *R. v. Giles*, [2007] B.C.J. No. 2918, 2007 BCSC 1147, 77 W.C.B. (2d) 469; *R. v. Harris* (2007), 87 O.R. (3d) 214, [2007] O.J. No. 3185, 2007 ONCA 574, 228 O.A.C. 241, 225 C.C.C. (3d) 193, 49 C.R. (6th) 220, 51 M.V.R. (5th) 172, 75 W.C.B. (2d) 492, 163 C.R.R. (2d) 176; *R. v. Law*, [2002] 1 S.C.R. 227, [2002] S.C.J. No. 10, 2002 SCC 10, 208 D.L.R. (4th) 207, 281 N.R. 267, J.E. 2002-325, 245 N.B.R. (2d) 270, 160 C.C.C. (3d) 449, 48 C.R. (5th) 199, 90 C.R.R. (2d) 55, 2002 D.T.C. 6789, [2002] G.S.T.C. 12, REJB 2002-27815, 52 W.C.B. (2d) 148; *R. v. Manley*, [2011] O.J. No. 642, 2011 ONCA 128, 275 O.A.C. 81, 269 C.C.C. (3d) 40; *R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 S.C.R. 281, [1993] S.C.J. No. 97, 157 N.R. 321, [1993] 8 W.W.R. 287, J.E. 93-1673, 12 Alta. L.R. (3d) 305, 145 A.R. 104, 84 C.C.C. (3d) 203, 24 C.R. (4th) 47, 17 C.R.R. (2d) 297, 20 W.C.B. (2d) 591; *R. v. Rodgers*, [2006] 1 S.C.R. 554, [2006] S.C.J. No. 15, 2006 SCC 15, 266 D.L.R. (4th) 101, J.E. 2006-910, 210 O.A.C. 200, 207 C.C.C. (3d) 225, 37 C.R. (6th) 1, 140 C.R.R. (2d) 1, 69 W.C.B. (2d) 741, EYB 2006-104246; *R. v. Spindloe*, [2001] S.J. No. 266, 2001 SKCA 58, [2002] 5 W.W.R. 239, 207 Sask. R. 3, 154 C.C.C. (3d) 8, 42 C.R. (5th) 58, 50 W.C.B. (2d) 11; *United States of America v. Carey*, 172 F.3d 1268 (10th Cir. 1999); *United States of America v. Tamura*, 694 F.2d 591 (9th Cir. 1982); *United States of America v. Turner*, 169 F.3d 84 (1st Cir. 1999)

Statutes referred to *Canadian Charter of Rights and Freedoms*, ss. 8, 24(2), *Criminal Code*, R.S.C. 1985, c. C-46, s. 489 [as am.], (a)-(c)

Authorities referred to Gold, Alan, "Applying Section 8 in the Digital World: Seizures and Searches" (presented at 7th Annual Six-Minute Criminal Defence Lawyer Program, Law Society of Upper Canada, Toronto, 2007)

Susan Magotiaux, for appellant.

Dale Ives, for respondent.

The judgment of the court was delivered by

BLAIR J.A.: -- Overview

[1] What happens when the police are lawfully searching a computer pursuant to a valid warrant for one crime and they discover evidence of another -- are they permitted to continue the computer search for further evidence of the second crime without another warrant? That is the essential question raised on this appeal.

[2] The police were investigating Mr. Jones for fraud. They believed he had participated in a fraudulent Internet scheme involving the sale of a motorcycle and that the invoice for the transaction was a computer-generated forgery. They obtained a warrant authorizing the search and seizure in his residence of data relating to certain e-mail transactions, images relating to counterfeit items and "[a]ny electronic data processing and storage devices, personal computer and computer systems". In the course of executing the warrant, they seized the appellant's computer, and in the course of examining its contents for evidence of fraud, they found evidence of child pornography.

[3] Without obtaining a further warrant -- and after seeking advice from an experienced Crown lawyer who advised they could proceed -- they continued their examination of the computer files in search of further evidence of pornography, including the search of video files that would not have been accessed had the search been confined to evidence of fraud. The result was the discovery of 57 images and 31 videos of child pornography.

[4] The respondent was charged with possession of child pornography. At his trial, Justice Nolan concluded that his rights under s. 8 of the *Canadian Charter of Rights and Freedoms* had been violated in the computer analysis because, although the warrant was valid for purposes of the fraud investigation, it did not authorize a review of the computer hard drive for anything other than evidence of fraud. She classified the advice given to the police as "reckless and cavalier", and symbolic of an institutional failure, and excluded the child pornography evidence found as a result of the search. The charges were therefore dismissed.

[5] The Crown appeals and "invites this Court to provide much-needed guidance on the appropriate scope of examination of computers seized under warrant". It also requests that we address what it characterizes as "the trial judge's unreasonable finding of recklessness" with respect to the Crown advice given to the police. [See Note 1 below]

[6] Although I agree with the trial judge that the search of the video files constituted a breach of the respondent's s. 8 rights, I would allow the appeal for the reasons that follow.

Facts

The initial investigation

[7] In November 2005, the respondent was under investigation for a fraud perpetrated through the use of a computer. The fraud related to the purchase of a Yamaha motorcycle listed for sale on e-Bay by a resident of Ogden, New York. In an e-mail, a person identifying himself as "Ronald Johnston" offered to buy the motorcycle, and in June 2005, a man using the same name went to Ogden and purchased the motorcycle using a Western Union money order. The money order turned out to be fraudulent, and the police suspected that it was a computer-generated forgery. The name "Ronald Johnston" also turned out to be a fake, but the e-mail address and e-Bay account were traced to Ronald Jones, the respondent, and to an address in London, Ontario.

[8] On November 19, 2005, the RCMP obtained a search warrant for the respondent's home. The terms of the warrant were broad and authorized the police to seize a number of things, including any computers and related equipment. For purposes of the appeal, the pertinent provisions are that the police were authorized to search the respondent's premises and to seize:

> -- All originals or copies of documents or data whether recorded on paper or as data stored within a computer system relating to the e-mail transmissions from Ronald Jones to James Holtz, [See Note 2 below] including but not limited to any e-mail address used by Ronald Jones including robjohnson_nysp @@Hotmail.com that contacted the victim James Holtz at this e-mail address mud4you[at]Rochester.rr.com or by any other means.
>
> -- Any electronic data processing and storage devices, personal computer and computer systems . . .
>
> -- Any documents . . . images, digital representations and templates of counterfeit tokens of value including but not limited to counterfeit Western Union money orders.

The review of the computer hard drives

[9] The warrant contained no restrictions on the types of computer files that could be searched. Before starting his inspection of the computer's two large hard drives, the police analyst, Sgt. Rimnyak, examined the relevant documentation and concluded that it was necessary to search all document and image files for evidence of fraud. Because the warrant contained no date limitation, he did not limit his search to any particular date range.

[10] During his initial review of the document and image files, Sgt. Rimnyak found images that he believed constituted child pornography, based on his previous experience with child pornography cases. He asked the investigating officer, Cpl. Herrington, to contact the Crown to determine whether a warrant should be obtained to search for further child pornography. The advice he received from Cpl. Herrington as a result of those inquiries was that, if there were no restricting terms or conditions in the warrant, the authorization permitted examination of the entire hard drive. Sergeant Rimnyak then contacted the Crown lawyer personally to ensure that the Crown understood that a full examination of the hard drives would include looking at video files that he would not have examined for purposes of the fraud investigation. Although he made no notes of the conversation, he testified that he received the

same advice, namely, that he could proceed without a further warrant to examine all files on the computer for evidence of child pornography.

[11] The full examination of the hard drives yielded the 57 images and 31 videos of child pornography referred to above.

The Crown advice

[12] Assistant Crown Attorney Fraser Kelly provided the impugned legal advice to Cpl. Herrington and Sgt. Rimnyak. Mr. Fraser is a seasoned Crown attorney, very experienced in matters relating to search and seizure. Having practised for 21 years, he was for 11 years a co-director of the search and seizure course at the Ministry of the Attorney General's summer "Crown School" attended by prosecutors from across the country. He was a designated wiretap agent and has lectured widely to lawyers and police on a variety of search and seizure issues. At the time, he was providing legal advice to police several times a week, most frequently with respect to those types of issues.

[13] Mr. Kelly did not specifically recall speaking with Cpl. Herrington or Sgt. Rimnyak but did not dispute that he likely gave them the "go ahead" advice that is questioned here. Indeed, it is not disputed that he did so. He could find no notes of his conversation but was not surprised by this because if the request were not by e-mail and was routine, he would not normally have a record. When providing advice by telephone, he did not routinely keep a notebook because he expected the police officers to do so.

[14] Mr. Kelly testified that "it is very probable that I would have advised them to proceed -- that provided the computer was lawfully placed in their hands for examination by a jurist, they were free to fully examine the entirety of its contents without obtaining a second section 487.01 warrant". He gave the police "the best advice regarding computer searches that [he] was able, with regard to the state of the law at the time". Corporal Herrington testified that Mr. Kelly referred to two cases in support of his advice; Crown and defence counsel agreed that those cases were *R. v. Law*, 2002 SCC 10 (CanLII), [2002] 1 S.C.R. 227, [2002] S.C.J. No. 10 and *R. v. Weir*, 2001 ABCA 181 (CanLII), [2001] A.J. No. 869, 156 C.C.C. (3d) 188 (C.A.). The trial judge ultimately took the position that those authorities did not support the advice given by Mr. Kelly. I will return to this discussion later in these reasons.

Analysis

[15] The overarching questions to be determined are whether the search for evidence of child pornography was authorized by the terms of the warrant itself or, if not, whether it was otherwise authorized in law and conducted in a reasonable manner. In that context, Ms. Magotiaux submits on behalf of the Crown that the trial judge erred in finding a breach of s. 8 of the *Charter*. She argues that (a) the warrant itself properly authorized seizure of the child pornography evidence because the police were entitled to make a full examination of the entire computer contents pursuant to it; (b) the manner of the search was reasonable for that reason and because the officer's conduct showed appropriate regard for the respondent's Charter rights; and (c) the "plain view doctrine" and s. 489 of the *Criminal Code*, R.S.C. 1985, c. C-46 apply in the computer context and support the legal search and seizure of the child pornography evidence in this case.

[16] In addition, she contends that the trial judge erred in impugning the advice provided by an experienced and knowledgeable Crown attorney and that this error fuelled the trial judge's decision to

exclude the child pornography evidence pursuant to s. 24(2) of the *Charter*, which, she submits, was an error as well.

[17] I will deal with each of these issues, but first I turn to a brief recital of the principles underlying s. 8 and search and seizure.

Underlying principles

[18] Section 8 of the *Charter* provides that "everyone has the right to be secure against unreasonable search or seizure". The general principles underlying that protection are well-established, but warrant repeating.

[19] A search and seizure is only lawful if it is authorized by law and if both the law and the manner in which the search is carried out are reasonable: *R. v. Collins*, 1987 CanLII 84 (SCC), [1987] 1 S.C.R. 265, [1987] S.C.J. No. 15, at p. 278 S.C.R.; *Law*, at para. 29. The onus is on the person seeking to establish the breach to show that his or her s. 8 rights have been violated. A warrantless search is prima facie unreasonable, however, and therefore a breach of s. 8, and the onus is on the Crown in such circumstances to prove that such a search was reasonable.

[20] To give effect to the s. 8 right involves an assessment in each case of whether the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals -- in particular, those related to law enforcement. The *Charter*'s bias is in favour of the former and, accordingly, in order to prevent unjustified searches, a legally valid pre- authorization, such as a warrant, is a pre-condition to a lawful search and seizure, where it is feasible to obtain one. See *Hunter v. Southam Inc.*, 1984 CanLII 33 (SCC), [1984] 2 S.C.R. 145, [1984] S.C.J. No. 36, at pp. 159-61 S.C.R.

[21] As *Hunter* and its progeny tell us, the primary value underpinning the s. 8 right is the need to protect an individual's reasonable expectation of privacy in the target of the proposed search against unreasonable intrusion by the state: see, also, for example, *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82, at pp. 426-27 S.C.R.; *R. v. Edwards* (1996), 1996 CanLII 255 (SCC), 26 O.R. (3d) 736, [1996] 1 S.C.R. 128, [1996] S.C.J. No. 11, at paras. 30 and 32; *R. v. Law*, supra, at paras. 15-16. The privacy expectation encompasses not only property interests, but personal and informational privacy too. As Bastarache J. observed in *Law*, at para 16:

> This Court has adopted a liberal approach to the protection of privacy. This protection extends not only to our homes and intimately personal items, but to information which we choose . . . to keep confidential.

[22] Here, we are concerned with the respondent's reasonable expectation as to his informational privacy. Sopinka J. defined the essential nature of this interest in *R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 S.C.R. 281, [1993] S.C.J. No. 97. At p. 293 S.C.R., he said:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. (Emphasis added)

Overview of analysis

[23] I have concluded that the trial judge was correct in holding that the warrant itself was valid for purposes of authorizing the search for evidence of fraud, but that it did not authorize a different search for evidence of child pornography other than that found in the data image files.

[24] This is not because the warrant should be struck as "too broad", in the sense that it contained no limitations on the ability of the police to search the computer, and therefore improperly invaded the high expectation of privacy the respondent had in the contents of his computer, as the respondent argues. It is because the warrant itself is properly restricted in the circumstances. Although it contained no limitations on the types of files that could be examined, it was reasonably focused and limited in the types of evidence the police could seek, and that evidence did not include evidence of child pornography.

[25] In addition, I do not accept the Crown's argument that the warrant authorized the search because a computer is an indivisible object which, like pieces of physical evidence, can be tested and inspected in whatever ways the police deem necessary once lawfully seized under the warrant. I also reject the somewhat connected suggestion that because the right to seize a computer would be a hollow one without the ability to examine its contents, it must follow that the police are entitled to examine the entirety of the contents.

[26] Accordingly, since the search for and seizure of evidence of child pornography was not authorized by warrant, it must be justified on some other basis. Here, the Crown relies on s. 489 of the *Criminal Code* and the operation of the common law "plain view" doctrine. These principles justify the seizure of the image files containing child pornography, but they do not justify the seizure of the video files containing child pornography in the circumstances. [See Note 3 below]

[27] Finally, with respect to s. 24(2) of the *Charter*, the trial judge erroneously based her decision to exclude the impugned evidence on a misapprehension of the evidence respecting systemic failure and on an unreasonable finding with respect to the nature of the Crown's advice. These errors re- open the analysis to this court and, in my view, the Grant analysis [See Note 4 below] favours inclusion of the evidence in the circumstances of this case.

[28] I turn now to a discussion of the issues.

The warrant itself did not authorize a search for child pornography

[29] I agree with the trial judge that the warrant was sufficient to support the search for evidence of fraud (using the word loosely -- more accurately, for evidence of possession of stolen property and evidence of uttering a forged document), but that it did not authorize the search for and seizure of the child pornography files. She said:

> With respect to whether the warrant was invalid, it is my view that the warrant was for a search for the offence related to the possession of stolen goods and the fraudulent use of a money order and was clear enough for that purpose. It was certainly not valid for the purposes of doing the further searches for child pornography.

[30] Whether the warrant was valid for the purposes of doing further searches for child pornography is dependent on the resolution of two conflicting points of view. Ms. Ives argued on behalf of the

respondent that the warrant was invalid on its face for such purposes because it was "too broad" in not placing any time or content limitations on the search of the computer. Ms. Magotiaux argued that the further search for child pornography was justified under the warrant because it placed no such limitations on the police, and rightly so since a computer, once lawfully seized, is like other physical objects that might yield evidence of crime and may be tested and inspected as the police deem necessary.

[31] I do not think either submission is correct.

Was the warrant "too broad"?

[32] First, I do not read the warrant as authorizing a comprehensive review of the entire contents of the appellant's computer without limitation. It is true that there are no parameters on the types of files that could be accessed or on the relevant time frame within which the police were entitled to examine the dated files on the computer. I do not see either of these factors as fatal, however.

[33] As noted above, the warrant places restrictions on the type of evidence that may be sought and is therefore not as broad and unlimited as may be suggested. It authorizes a search and seizure in respect of evidence of fraud. And in respect of fraud, it is relatively focused in its reach: it permits a search in the respondent's residence for, and the seizure of (i) any personal computers and related equipment or devices (the "computers"); (ii) data stored within a computer system relating to e-mail transmissions between the respondent and the seller of the motorcycle; and (iii) any documents, images or digital representations of counterfeit tokens of value, including, but not limited to, counterfeit Western Union money orders. In effect, the warrant contemplated a two-staged search: first, for the computer and related devices; and secondly, a search of the contents of the computer for evidence relating to the e-mail transmissions and the counterfeit images in question. This is not too broad.

[34] Ms. Ives further submits that the warrant is invalid on its face because it does not place any constraints on the relevant time frame within which the police were entitled to examine the dated files on the computer: see *R. v. Du*, [2004] A.J. No. 1324, 2004 ABQB 849, at paras. 16-22. I do not think much turns on this omission here, however, because the warrant is quite clear and focused with respect to the targets of the computer search, i.e., data stored within the computers systems relating to the described e-mail transmissions and images, digital representations and templates of counterfeit tokens. Date parameters are not particularly pertinent to that inquiry and their absence does not allow the police authorities to stray beyond the legitimate targets of the search. The warrant is not overly broad in this respect either, in my opinion.

The nature of a computer search

[35] Much energy and argument were devoted at trial and on appeal to the nature of a computer in the context of a search of its contents. The respondent trumpeted the almost unlimited amounts and variety of personal and confidential information that may be stored on an individual's computer, and the need to protect the individual's s. 8 reasonable expectation of privacy in such information to the extent possible in the course of a search of the computer's contents. The Crown emphasized the need for broad search parameters for a series of practical reasons that I will address and also took the position that, once lawfully seized, a computer, like other physical objects, could be subjected to whatever tests may be necessary: the right to seize a computer is hollow without the right to search its contents.

[36] There are compelling arguments to be made for all of these positions but, in the end, I do not accept that the broad right to examine all computer contents in search of evidence of fraud pursuant to the warrant was sufficient to authorize a further search for evidence of child pornography without the police obtaining a second warrant. This could easily have been done. Searches of this nature are generally performed off-site and post-seizure, as this one was. Frequently, as here, there is no urgency. In such circumstances, nothing prevents the police from applying for another warrant.

The computer as repository of confidential information

[37] In this debate, there is a common recognition that computer searches are invasive and that computers are the repository of immeasurable and infinitely variable chunks of highly private and confidential personal information -- often the very epitome of the type of "biographical core" information sought to be protected by the privacy expectations underlying s. 8. Justice Fish captured this notion vividly in *R. v. Morelli*, 2010 SCC 8 (CanLII), [2010] 1 S.C.R. 253, [2010] S.C.J. No. 8, at paras. 2-3:

> 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.
>
> First, police officers enter your house, 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.

[38] This is more or less what happened to the respondent's computer, and Ms. Ives submits that a warrant issued to search a computer for one valid purpose cannot justify an expanded search for a different purpose, given the high expectation of privacy that a person has in the contents of his or her computer.

The Crown's practical concerns

[39] On the other side of the ledger, prosecutorial authorities -- including the appellant in this case -- raise a number of concerns about the nature of computer evidence that militate in favour of more broadly worded and flexible authorizations in this area. They point to (a) the difficulty in narrowing the field of search, given the realities of developing technology and the recognized ability of individuals to conceal information by storing it in different fashions, and by manipulating and reorganizing it so that a simple viewing of folder names and file lists or extensions may not provide an accurate reflection of the information stored in them; (b) the fact that a warrant is issued (often very early) at the investigatory stage, and it is not practical at that stage to be precise about what could be relevant evidence; (c) the fact that investigators, when making out grounds for a warrant, may not have the advance knowledge of what they will be examining or how they may be able to access the information stored on the computer, given the fast-paced nature of developing technology; and (d) the difficulty that judicial officers face in assessing the suitability of technological search parameters that may be put forward in a wide variety of personal electronic device seizures.

[40] There may be valid reasons, then, why the language used to authorize computer searches may need to be relatively broad in order to cope with the practical realities of an ever- changing and developing age of technology. That said, there must also be some counter-balance to protect the privacy rights of individuals in the contents of their computers. All rights to privacy in the contents of a computer need not be trampled on to achieve the state's law enforcement objectives in a reasonable fashion.

[41] At one level, it is true to say that the authorization to search for and seize a computer is hollow unless the police have the corresponding right to examine its contents. As A.W. MacKenzie J. observed in *R. v. Giles*, [2007] B.C.J. No. 2918, 2007 BCSC 1147, at para. 56, "[a computer] device [is] meaningless without its contents". But, the question is, what is the proper scope of that corresponding right to examine?

[42] I do not accept that the right to examine the entire contents of a computer for evidence of one crime (fraud, in this case) carries with it the untrammelled right to rummage through the entire computer contents in search of evidence of another crime (possession of child pornography, in this case) without restraint -- even where, as here, the warrant may properly authorize unlimited access to the computer's files and folders in order to accomplish its search objectives. A computer search pursuant to a warrant must be related to the legitimate targets respecting which the police have established reasonable and probable grounds, as articulated in the warrant.

[43] Here, that focus has been accomplished not by limiting access to the contents of the computer but -- as described above -- by framing the type of evidence that may be sought (evidence relating to the e-mail transmissions and to counterfeit images) and the crimes to which that evidence relates (possession of stolen property and forgery). The focus on the type of evidence being sought, as opposed to the type of files that may be examined is helpful, it seems to me, particularly in cases where it may be necessary for the police to do a wide-ranging inspection of the contents of the computer in order to ensure that evidence has not been concealed or its resting place in the bowels of the computer cleverly camouflaged.

[44] To the extent they are required to examine any file or folder on the computer to reasonably accomplish that authorized search, the police are entitled to open those files and folders and to examine them, at least in a cursory fashion, in order to determine whether they are likely to contain evidence of the type they are seeking: see, for example, *R. v. Manley*, [2011] O.J. No. 642, 2011 ONCA 128, at para. 38; *United States of America v. Williams*, 592 F.3d 511 (4th Cir. 2010), at pp. 521-22 F.3d, cert. denied *Williams v. United States of America*, 131 S. Ct. 595, 178 L. Ed. 2d 434 (2010).

One seizure fits all

[45] A central theme in the Crown's argument was the notion of the computer as an indivisible object of search. On this view, a computer is an item to be seized and, like any other physical object lawfully seized, is subject to whatever testing the police may determine necessary -- even with respect to subsequently discovered crimes. For example, a suspect's clothing seized under a warrant in a sexual assault investigation may later be tested for semen in the context of a subsequent murder investigation: see *R. v. DeJesus*, [2010] O.J. No. 3744, 2010 ONCA 581, at paras. 5-10. Body samples (scalp and pubic hair) given on consent with a view to eliminating an individual as a suspect in one murder case were properly tested for a DNA match in connection with a second murder: *R. v. Arp*, 1998 CanLII 769 (SCC), [1998] 3 S.C.R. 339, [1998] S.C.J. No. 82, at paras. 82-90. See, also, *R. v. Rodgers*, 2006 SCC 15 (CanLII),

[2006] 1 S.C.R. 554, [2006] S.C.J. No. 15, at para. 43; *R. v. Dore*, 2002 CanLII 45006 (ON CA), [2002] O.J. No. 2845, 166 C.C.C. (3d) 225 (C.A.), at para. 50. The rationale behind this concept is that no reasonable expectation of privacy remains in the object once an object has been lawfully obtained by the police for the purpose of criminally investigating the suspect.

[46] Put in the terms of this case, the argument is that a warrant containing no limiting terms with respect to the parts of the computer that could be searched, properly authorizes a full examination of all the data stored on the computer as if it is one indivisible item. I do not accept this view, however. In my opinion, the analogy between forensic testing of a physical object and the examination of the contents of a computer is not an apt one. Unlike a physical object, it is not information generated by the physical characteristics of or adhering to the object that is the target of the search. It is the informational contents of the computer themselves that are the target of the search. This is a qualitative difference.

[47] A better analogy is to the search and seizure of two different "places": the home in which the computer is found, for example, and the computer itself.

[48] A home contains all kinds of rooms, closets, cabinets, drawers, folders, files, safe vaults and the like. Each may be a cache for a limitless variety of personal "biographical core" information. The same may be said for computers. Vast amounts of personal information are stored in data banks. Although the technology underlying these concepts is complex, documents, images, audio files, videos and other digital representations are stored on "drives" and are organized in "folders", "sub- folders" and "files." Files themselves are characterized by various "extensions", signifying their type.

[49] Thus, authorizing a search of the contents of a computer is not unlike authorizing a search of another "place" or of a more expansive search of the same "place". There seems to me to be no reason in principle why the state should be any more entitled to roam around through the contents of a person's computer in an indiscriminate fashion than it would be to do so in a person's home without further authorization.

[50] The police have available to them the necessary software, technology and expertise to enable them to tailor their searches in a fashion that will generate the information they seek, if it exists, while at the same time minimizing the intrusion on the computer user's privacy rights in other information stored on the computer. Sergeant Rimnyak testified that the EnCase software used in this case permits the police to view all data and all files contained on the computer, but that the police do not normally look at all files in the course of an investigation; they focus on those they think will generate the evidence they are looking for. That is as it should be.

[51] As noted above, computers are different from other more traditional objects of search and seizure. They are different not only because of the inordinately vast amounts of personal information that can be stored on them, but also -- in the words of Fish J. in *Morelli* -- because of the electronic roadmap they can provide with respect to the "cybernetic peregrinations" of the individual whose computer it is. They are different as well because of the technological difficulties inherent in the ability of prosecutorial authorities to search precisely for what they are entitled to obtain. For the most part, however, these differences are in the degree and quantum of information that may be accessible on searching a computer, as opposed to searching, for instance, a home. Or, they are simply differences in methods and mechanisms used to access the information (complex and sophisticated software and technology in the case of computers, and the more prosaic human senses of sound, sight, touch and smell aided by

forensic science in the case of traditional searches). These differences are not differences in principle. Stripped to their essentials for these purposes, conceptually, computers -- like homes -- are simply the storage repositories for a great deal of information about an individual (albeit often sensitive private and confidential information).

[52] In conclusion, I do not accept the Crown's theory of the computer as an indivisible object for these purposes. Nor, based on all of the foregoing, do I accept that the warrant issued here, itself, authorized a further warrantless search for evidence of child pornography.

The "plain view" doctrine and s. 489

[53] The next issue does not concern whether the warrant was "valid for purposes of doing further searches for child pornography". Indeed, no one ever anticipated that the warrant would encompass a search for child pornography. The issue is the extent to which the discovery of evidence pointing to a second (and unanticipated) crime can piggyback onto the lawful execution of a computer-search warrant directed at a different crime. More specifically, the issue is whether, having lawfully conducted a search of data and image files for evidence of fraud, and having discovered image files containing what they reasonably believed to be child pornography, the police were (a) entitled to seize and utilize the image files containing child pornography to form the basis for a child pornography investigation and prosecution (a different offence than the one for which they were lawfully seeking evidence); and (b) entitled to conduct a further examination of other computer files for further evidence of child pornography, including video files that they would not have examined in the course of their search for evidence of fraud, for the same secondary purpose.

[54] The answers to these questions depend upon the applicability of the plain view doctrine and of s. 489 of the *Criminal Code* to the facts of this case.

[55] The Crown submits the plain view doctrine and/or s. 489 of the *Criminal Code* justify both the search and seizure of the images of child pornography discovered by Sgt. Rimnyak during his first review of the computer files and of the videos of child pornography found in the subsequent search. I agree that they justify the former, but do not accept that they justify the latter.

[56] The "plain view" doctrine operates when a police or peace officer is in the process of executing a warrant or an otherwise lawfully authorized search with respect to one crime and evidence of another crime falls into plain view. Resort to this common law power is subject to the following restraints, however: (i) The officer must be lawfully in the place where the search is being conducted ("lawfully positioned", in the language of the authorities); (ii) the nature of the evidence must be immediately apparent as constituting a criminal offence; (iii) the evidence must have been discovered inadvertently; (iv) the plain view doctrine confers a seizure power not a search power; it is limited to those items that are visible and does not permit an exploratory search to find other evidence of other crimes. See, generally, *R. v. Spindloe*, 2001 SKCA 58 (CanLII), [2001] S.J. No. 266, 154 C.C.C. (3d) 8 (C.A.), at pp. 29-37 C.C.C.; *R. v. F. (L.)*, 2002 CanLII 45004 (ON CA), [2002] O.J. No. 2604, 166 C.C.C. (3d) 97 (C.A.), at paras. 28-34; *Law*, *supra*, at para. 27, and the authorities cited therein.

[57] Section 489 of the *Criminal Code* states:

> 489(1) Every person who executes a warrant may seize, in addition to the things mentioned in the warrant, any thing that the person believes on reasonable grounds

> (a) has been obtained by the commission of an offence against this or any other Act of Parliament;
>
> (b) has been used in the commission of an offence against this or any other Act of Parliament; or
>
> (c) will afford evidence in respect of an offence against this or any other Act of Parliament.
>
> (2) Every peace officer, and every public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties may, without a warrant, seize any thing that the officer believes on reasonable grounds
>
> (a) has been obtained by the commission of an offence against this or any other Act of Parliament;
>
> (b) has been used in the commission of an offence against this or any other Act of Parliament; or
>
> (c) will afford evidence in respect of an offence against this or any other Act of Parliament.

[58] Both the common law plain view doctrine and the statutory s. 489 provisions are exceptions to the general rule that a warrantless search is unreasonable and, therefore, a violation of s. 8. Some have suggested that s. 489 is a codification of the plain view doctrine. I note that Borins J.A. expressed doubt about that proposition in *F. (L.)*, at para. 22. While it is not necessary to decide that issue here, I, too, am not persuaded that such is the case. See, also, *R. v. B. (E.)*, [2011] O.J. No. 1042, 2011 ONCA 194, at paras. 75-78.

[59] Whether the plain view doctrine should apply in circumstances involving a computer search has been a matter of much debate. The debate has centred on the intrusive nature of computer searches and the somewhat awkward fit between traditional search and seizure concepts and computer technology. In *R. v. Bishop*, [2007] O.J. No. 3806, 2007 ONCJ 441, for example, R.D. Clarke J. posed an example which is the converse of this one, namely, where police are searching for evidence of child pornography but come across evidence relating to an otherwise unknown fraud. At para. 37, he observed that "the concepts of plain view would seem to provide the police with a legitimate justification for their conduct", but commented that there was, in his view, "good reason to question whether this approach [would] survive". He went on to frame the concern in this way, at paras. 38-39:

> The search and seizure of mass storage devices tests the "reasonableness" of plain view when applied to the context of computer crime investigations. Justifiable searches will often require sweeping examinations of all data on a hard drive. Where the circumstances of the particular investigation justify such a wide-ranging search (for example, where evidence suggests that the target of the search has used "countermeasures" to secrete seizable data in or disguised as, other files), then no issues should arise.

> Where, however, police routinely seize and review all material on a hard drive, even if they know only a small percentage is likely to be responsive to the warrant then constitutional issues are engaged. So far as I am aware at present these issues remain unresolved.

[60] In the United States, there has been a similar discussion. *United States of America v. Comprehensive Drug Testing Inc*., 579 F.3d 989 (9th Cir. 2009), revised 621 F.3d 1162 (9th Cir. 2010), is perhaps the fullest example of the debate. There, the federal government was conducting an investigation into the use of steroids by professional baseball players. The Major League Baseball Players Association agreed that players would submit to urine samples solely for the purpose of determining the percentage of positive results; the results themselves were to remain confidential. When ten players tested positive, however, the government obtained warrants to obtain information from private entities that had collected the samples and information. Comprehensive Drug Testing Inc. was one of those entities. The warrants were limited to information about the ten players respecting whom there was probable cause to believe had engaged in steroid use; however, the government seized and reviewed drug-testing records of hundreds of players and many other people stored on the computers of the drug-testing providers. The warrants were quashed and the seized property ordered returned.

[61] The government was successful on its initial appeal to the Ninth Circuit; however, the judges of that court agreed to rehear the case en banc. After the en banc hearing, the judges split on whether the state should be able to rely upon the plain view doctrine in cases involving a computer search. Indeed, the court took the unusual position of issuing a revised en banc opinion a year later, in which it appears to have softened its first (majority) view that the government should "forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data" (p. 998 F.3d). In a sentiment somewhat similar to that expressed by Fish J. in *Morelli*, the majority in the first en banc opinion justified that view by framing the risks in this way, at pp. 998 and 1004-1005 F.3d:

> The point of the Tamura [See Note 5 below] procedures is to maintain the privacy of materials that are intermingled with seizable materials and to avoid turning a limited search for particular information into a general search of office file systems and computer databases. If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file -- and we have no cavil with this general proposition -- then everything the government chooses to seize will, under this theory, automatically come into plain view. Since the government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less: Why stop at the list of all baseball players when you can seize the entire Tracey Directory? Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been. . . . Let's take everything back to the lab, have a good look around and see what we might stumble upon. [See Note 6 below]

[62] The majority went on later to elaborate on this general theme, at pp. 1004-1005 F.3d:

> The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents -- either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among

> which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.
>
> Once a file is examined, however, the government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search some computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media. Where computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there.

[63] Not all U.S. courts have accepted the *Comprehensive Drug Testing Inc.* approach to plain view, however. For example, *United States v. Williams*, *supra*, involved an authorized search for evidence of the crimes of threatening and computer harassment during which evidence of child pornography was found and seized. In upholding the seizure, the Fourth Circuit Court of Appeal acknowledged the proper application of the doctrine in the computer search context, explaining it is this way (at p. 522 F.3d):

> Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain- view exception are readily satisfied. First, an officer who has legal possession of the computer and electronic media and a legal right to conduct a search of it is "law-fully present at the place from which evidence can be viewed," thus satisfying the first element of the plain-view exception. Second, the officer, who is authorized to search the computer and electronic media for evidence of a crime and who is therefore legally authorized to open and view all its files, at least cursorily, to determine whether any one falls within the terms of the warrant, has "a lawful right of access" to all files, albeit only momentarily. And third, when the officer then comes upon child pornography, it becomes "immediately apparent" that its possession by the computer's owner is illegal and incriminating. And so, in this case, any child pornography viewed on the computer or electronic media may be seized under the plain-view exception. (Emphasis in original; citations omitted)

[64] In the foregoing debate, I prefer the general view articulated by the Fourth Circuit. As noted above, this court adopted the "cursory review" approach in *Manley*, *supra*, where the police conducted a cursory search of a cellphone seized incident to arrest. Moreover, I do not think it can be said that, because information on a computer is not visible to the human eye, but requires the use of a software program to access it, it is not in "plain view". Once a file is opened by the computer programmer using the software, its contents can be read, and "plain view" comes into play, as the court noted in *Williams*.

[65] Here, I am satisfied that the Crown's reliance on the child pornography found in the image files discovered in the course of the initial search for fraud-related evidence in this case does not violate s. 8. Sgt Rimnyak was lawfully examining the image files under the warrant when he unexpectedly saw images that were immediately recognizable as images of child pornography. Thus, his detection of the child pornography images in those files met all the requirements of both the plain view doctrine and s. 489 of the *Criminal Code*. He was entitled to seize them.

[66] For a number of reasons, however, the same cannot be said about the video images of child pornography.

[67] First, the video files were not sitting "in plain view" following the discovery of the child pornography image files and, while the plain view doctrine authorized Sgt. Rimnyak to seize those image files, as noted above, it did not authorize him to conduct a further exploratory search for other evidence of child pornography. Secondly, the videos were not inadvertently or unexpectedly discovered during the subsequent search he did conduct. Sergeant Rimnyak suspected he might find more evidence of child pornography if he did the further search, and he was deliberately looking for that evidence. The doctrine therefore did not apply. Finally, to permit the plain view doctrine to operate in such circumstances would be to run the risk of overseizure, a risk to which electronic media searches are particularly susceptible and something the court must guard against: see Bishop, supra.

[68] In his presentation to the 7th Annual Six-Minute Criminal Defence Lawyer Program sponsored by the Law Society of Upper Canada, entitled "Applying Section 8 in the Digital World: Seizures and Searches", Alan Gold aptly described the dangers of adopting the plain view doctrine uncritically to the computer world, including the problem of overseizure. At p. 3-2, he said:

> Overseizure is a particularly acute problem in the digital context because by its very nature a computer contains massive amounts of information on topics and matters as diverse as an owner's life. Further, the "plain view" doctrine may have much greater scope to operate if a police officer is entitled to search at will through every nook and cranny of the computer. The information in a computer is not in a form accessible to the human eye without using the computer itself, and the very act of computer use may arguably allow, if not require, law enforcement access to information and data outside the terms of the search warrant. In many ways a search warrant for a computer is really like the old general warrants or writs of assistance which authorized searches at large.

[69] Various American authorities have expressed similar views. See, for example, *United States of America v. Carey*, 172 F.3d 1268 (10th Cir. 1999), at p. 1273 F.3d (police officer finding evidence of child pornography while looking for evidence of drug trafficking); *United States of America v. Turner*, 169 F.3d 84 (1st Cir. 1999), at p. 88 F.3d (officer finding evidence of child pornography while in search of evidence regarding an assault); *United States v. Comprehensive Drug Testing Inc.*, *supra* (evidence of steroid use by a large number of Major League Baseball players and many others discovered while searching for steroid use by ten players with respect to whom reasonable and probable grounds existed).

[70] For these reasons, I would not extend the plain view doctrine to justify the police seizure and ensuing use by the Crown of the subsequently discovered video files.

[71] Nor does s. 489 of the *Criminal Code* assist in this respect. For the purposes of this case, its reach stops as well at the discovery of the image files.

[72] There is very little jurisprudence dealing with s. 489. In *F. (L.)*, at para. 27, Borins J.A. concluded, after a brief consideration of the section, that

> . . . the power of seizure which [subsections (1) and (2)] authorize necessarily is confined to what police officers locate in the execution of a valid search warrant under subsection (1) or where an officer is lawfully present in a place under subsection (2). Therefore, read as a whole, s. 489

> authorizes police officers to lawfully seize items which they locate in the circumstances provided for in subsections (1) and (2).

[73] Implicit in the s. 489 power is the premise that the law enforcement officer has come across or seen something in the course of a lawful search. The law enforcement officer must have reasonable and probable grounds to believe that that something "will afford evidence" of a crime. [See Note 7 below] For the reasons expressed above, Sgt. Rimnyak did not come across or see the video files in the course of his initial seizure and search of the computer. Like the plain view doctrine, s. 489 provides law enforcement agencies with a right to seize. It does not provide them with a right to search for further evidence.

[74] Section 489, therefore, does not apply.

Section 24(2)

[75] I have concluded that the seizure of the image files containing child pornography did not constitute a breach of the respondent's s. 8 *Charter* rights. It follows that those image files are admissible and that no s. 24(2) issue arises in respect of them. Given the contrary conclusions respecting the seizure of the video files containing child pornography, however, the trial judge's decision to exclude that evidence pursuant to s. 24(2) must be considered.

[76] Section 24(2) of the *Charter* provides that:

> 24(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this *Charter*, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

[77] The principles to be applied when assessing whether evidence should be excluded under s. 24(2) have recently been re-formulated by the Supreme Court of Canada in *R. v. Grant*, supra, at paras. 67-71. In summary, the court is to consider (1) the seriousness of the *Charter* breach, (2) the impact of that breach on the accused's *Charter*-protected rights and (3) the societal interest in having criminal matters adjudicated on their merits. If, on a proper application of these principles, and having regard to all of the circumstances, the court is satisfied that admitting the evidence would bring the administration of justice into disrepute -- taking a long-term view of this notion -- the court is required to exclude the tainted evidence. The decision is discretionary and generally attracts a great deal of deference.

[78] Here, the trial judge addressed those proper principles. Respectfully, however, her decision to exclude the evidence of child pornography is tainted by two significant evidentiary missteps. Her finding that the Crown's advice to the police to proceed without a further warrant was, amongst other things, "cavalier or reckless" was, in my view, both unnecessary and unwarranted on the record. In addition, her finding -- built on this conclusion -- that the Crown's error indicated a systemic problem or failure is not supported by any evidence.

[79] Where a decision to exclude evidence under s. 24(2) "is tainted by an error in principle, a misapprehension of material evidence, or is arrived at by virtue of an unreasonable assessment of the evidence, the resulting exclusion of the evidence will constitute an error of law appealable by the Crown": *R. v. Harris* (2007), 2007 ONCA 574 (CanLII), 87 O.R. (3d) 214, [2007] O.J. No. 3185, 225 C.C.C.

(3d) 193 (C.A.), at para. 51. Put another way, where a s. 24(2) decision is based on such errors it is no longer entitled to the considerable deference that normally attaches to such a decision, and the s. 24(2) analysis is re-opened afresh for the appellate court's consideration. That is the case here. I turn first, though, to the errors I have just mentioned.

[80] The trial judge was unconsciously ensnared, I think, by her overblown criticism of the Crown's advice. Her view that the Crown's advice was "cavalier or reckless", or at least careless or negligent and that it demonstrated a "clear disregard" for the respondent's s. 8 rights was simply unfounded on the record, in my respectful opinion. The genesis for this view of the Crown's advice appears to be two-fold: the trial judge thought the advice was wrong, and she was particularly influenced by the fact that neither Sgt. Rimnyak nor Mr. Kelly took notes of their conversation.

[81] I confess, I do not understand the relevance of this latter fact, but it seems to have taken on a life of its own in the case. No one is disputing that Mr. Kelly gave the go-ahead advice that he is said to have given. What else mattered about the conversation (which might well be protected by solicitor/ client privilege, in any event) for these purposes? The police were only interested in the advice on whether to proceed or not to proceed. Mr. Kelly was surely not expected to give a memorandum-of-law dissertation to Sgt. Rimnyak and Cpl. Herrington about the pros and cons of the jurisprudence he considered in arriving at his recommendation, and record that dissertation. While it would have been preferable if he had made notes of the discussion -- as the Crown's guidelines provided -- I fail to see what turns on his failure to do so in these circumstances. If the tenor of the advice he had given was at issue, it might be different. But it was not.

[82] Mr. Kelly testified that he gave "the best advice regarding computer searches that [he] was able [to give], with regard to the state of the law at that time". The trial judge made no finding that she did not accept this evidence. Indeed, she did not refer to it.

[83] Ms. Ives concedes that "the general law relating to computer searches was and remains unsettled", but she argues that "the inapplicability of the plain view doctrine to the video files was obvious". [See Note 8 below] Although I have concluded that the plain view doctrine could not justify the seizure of those files, I do not think the conclusion that the police were entitled to proceed without a further warrant was so "obvious" at the time the Crown's advice was given (or, indeed, before this decision by the trial judge).

[84] The advice was given in November 2005. At that time, both the Alberta Court of Appeal's decision in *R. v. Weir*, supra, and the decision of the Ontario Superior Court in *R. v. Lefave*, [2003] O.J. No. 3861, [2003] O.T.C. 872 (S.C.J.) provided some support for Mr. Kelly's opinion. In *Weir*, the police had a warrant to seize a computer and did so. Without placing any limitation on the data extraction or analysis that could be permitted, the court simply stated, at para. 19, that "[a]s long as the CPU was properly seized, the information contained in it could be extracted at a later date" (emphasis added). In *Lefave*, the police seized a laptop computer incident to an arrest for communicating a threat over the Internet, and while searching the computer found evidence of child pornography. They sought advice from the Crown, who told them they could proceed without a warrant. Dunn J. gave credence to this advice when he found no s. 8 breach, relying on the plain view doctrine to do so.

[85] There was no appellate authority at the time governing the application of the plain view doctrine or of s. 489 of the *Criminal Code* in the computer search context. *Morelli* had not yet been decided, nor had the American authorities such as *United States v. Comprehensive Drug Testing Inc.* or *United States v. Williams*, mentioned above. Even later, in 2007, Justice Clarke of the Ontario Court of Justice acknowledged that "justifiable searches will often require sweeping examinations of all data on a hard drive" and noted that the limitations on such searches remained unresolved: *Bishop*, at paras. 38-39. And in *Giles*, the British Columbia Supreme Court permitted the search of the entire contents of a Blackberry seized incidental to an arrest on the theory that "[the] device was meaningless without its contents" and that "[o]nce an item is seized for use in a criminal investigation, the police are entitled to subject it to technical analysis to determine its evidentiary significance": paras. 56-57.

[86] Although the law has evolved to the point where the Crown's advice in this case has turned out to be wrong, it does not follow that this ought to have been "obvious" from the beginning and that the Crown's advice was negligent, reckless or in wilful disregard of the respondent's *Charter* rights. To the contrary, the advice had some support in the authorities and cannot be said to have been unreasonable at the time, in my view. It simply turned out to be incorrect.

[87] Thus, while the Crown's advice may have been "unsound", in the sense that it ultimately turned out to be erroneous in the circumstances, the findings that it was "cavalier or reckless" or at least negligent and that it demonstrated "a clear disregard" for the respondent's s. 8 rights are simply unreasonable on this record.

[88] The trial judge compounded her error in this regard by jumping from her view that the Crown's advice was "cavalier or reckless" to her conclusion that this represented a systemic failure in the office of the Crown. There was no evidence to support this jump. The Crown had a guideline in place for dealing with consultations between Crown attorneys and police respecting warrants (albeit one not followed in this particular case, in terms of note-taking). The Crown consulted was a senior Crown with a great deal of experience in the field. There is no suggestion in the record of any other incident -- much less widespread incidents justifying the use of the word "systemic" -- where the Crown's advice in such circumstances had been found wanting (indeed, in *LeFave* it appeared to have been vindicated).

[89] Yet the trial judge concluded that "the fact that an error occurred suggests a systemic problem or failure". She went on almost immediately to observe that "systemic failures are precisely the type of concerns that s. 24(2) is aimed at" and to her final determination that, although it was not at the extreme end of the spectrum, the breach was "still a serious infringement" of the respondent's s. 8 rights.

[90] These mistaken views moved the trial judge towards excluding the evidence. They played a critical role both in her assessment of the seriousness of the breach (the first *Grant* factor) and in the ultimate balancing of all three factors in determining whether admitting the impugned evidence would bring the administration of justice into disrepute. Because they undermined her conclusions in principle, the s. 24(2) analysis must be reconsidered by us. Having considered all the factors and circumstances, I arrive at a different conclusion than did the trial judge. For the reasons that follow, I would not exclude the video files containing child pornography from the evidence.

The seriousness of the breach

[91] I accept that the *Charter* breach was somewhat serious, given the heightened expectation of privacy the jurisprudence demonstrates an individual enjoys in the contents of his or her computer: see *Morelli*, at paras. 1 and 99. That said, I do not agree that the search was as egregious a breach as the trial judge made it out to be.

[92] On this record, the conduct of the police cannot be said to be anything other than conduct carried out in good faith. Sergeant Rimnyak was meticulous in seeking the advice he needed before proceeding. He initially asked the investigating officer, Cpl. Herrington, to make inquiries of the Crown, and even when she reported that he was entitled to go ahead with the full search he went back to the Crown and spoke to Mr. Kelly himself in order to ensure that the technical nature of what was involved was understood. The police, who had originally gone in with a warrant, believed they had the lawful authority to continue without obtaining a fresh warrant.

[93] For the reasons outlined above, I do not accept that the Crown acted in bad faith. Indeed, I do not think that, simply because the advice the Crown gave turned out several years later to be incorrect in law, the Crown was not acting in good faith. Legal opinions are crafted every day that turn out to be unsupported when the subject matter of the opinion ultimately gets to trial. It does not follow that the authors of those opinions were not acting in good faith when they provided them.

[94] Although, as I have said, the breach was somewhat serious, it was more akin to the breach described by Fish J. in *Morelli*, at para. 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.

[95] The seriousness of the breach factor favours admission of the evidence in this case.

The impact of the breach

[96] The breach had considerable impact on the *Charter*-protected rights of the respondent, however. For this part of the analysis, the intrusion upon the respondent's reasonable expectation of privacy in the portions of the computer contents the police were not entitled to search takes on particular significance. The reasonable expectation is very high. Therefore a violation of it is very serious.

[97] I have already rejected the Crown's argument that an individual loses all reasonable expectation of privacy in a computer once -- as in the case of a physical object -- it is lawfully seized. Computers are very different, as the jurisprudence has made clear. Nor do I accept that there is a significantly reduced expectation of privacy in the contents of the computer that police are not entitled to examine because of a prior lawful seizure of the computer entitling the police to search other parts of the contents. An individual does not lose his or her reasonable expectation of privacy in places in a home that police are not lawfully entitled to search. Computer contents are no different for these purposes, in my opinion.

[98] Thus, the impact of the breach on the *Charter*-protected s. 8 rights of the respondent is significant here. This weighs in favour of exclusion of the evidence.

Society's interest in a trial on the merits

[99] Turning to the third part of the Grant analysis, society's interest in having serious criminal allegations adjudicated on their merits is also high. The evidence is important to the Crown's case, although the Crown will still be able to proceed with charges arising out of the image files seized. The evidence is real, not conscripted, and it is reliable.

[100] These factors weigh in favour of not excluding the evidence at trial.

Balancing the criteria

[101] At the end of the day, the *Grant* approach requires a determination of whether the administration of justice would be brought into disrepute by the inclusion of the impugned evidence. It is the long-term view of this notion that counts, not society's unconsidered reaction to a particular case. As McLachlin C.J.C. and Charron J. noted in *Grant*, at para 68:

> The phrase "bring the administration of justice into disrepute" must be understood in the long-term sense of maintaining the integrity of, and public confidence in, the justice system. Exclusion of evidence resulting in an acquittal may provoke immediate criticism. But s. 24(2) does not focus on immediate reaction to the individual case. Rather it looks to whether the overall repute of the justice system, viewed in the long term, will be adversely affected by admission of the evidence.

[102] Two of the three Grant criteria work in favour of not excluding the video files, in my opinion. Balancing the factors is not simply a mathematical exercise. However, I am satisfied in all the circumstances that the administration of justice would be brought into disrepute more, in the long-term, if the video file evidence is excluded rather than included. The police acted in good faith throughout, believing they had the lawful right to continue their search of the computer. While the Crown's advice turned out to be incorrect in the end, the Crown did not fail to act in good faith. Crimes involving child pornography are among the most abhorrent in society. Society's interest in having these charges tried on their merits, with the important, reliable and real evidence that is available being tendered, is very high.

[103] Balancing all of the factors, I would not exercise the court's discretion to exclude the evidence of child pornography contained in the video files seized in contravention of the respondent's s. 8 *Charter* rights. Disposition

[104] For the foregoing reasons, I would allow the appeal, set aside the acquittal and order a new trial.

[105] In closing, I would like to thank counsel for their helpful presentations and materials in this difficult case.

Appeal allowed.

Notes

Note 1: Appellant's factum, paras. 4 and 59.

Note 2: The seller of the motorcycle.

Note 3: The witnesses distinguished between "image files" and "video files" for the purposes of this proceeding. By adopting that terminology in these reasons, I do not mean to suggest that video files may not contain images from a technical perspective.

Note 4: *R. v. Grant*, 2009 SCC 32 (CanLII), [2009] 2 S.C.R. 353, [2009] S.C.J. No. 32, at paras. 67-71.

Note 5: *United States of America v. Tamura*, 694 F.2d 591 ((9th Cir. 1982), at pp. 595-96 F.2d. *Tamura* holds that where relevant and irrelevant documents are intermingled, the police must engage in an intermediate step of sorting various types of documents and then only searching the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. Whether an intermediate-step approach should be adopted in this jurisdiction is not an issue that needs to be decided in this case.

Note 6: This passage and the one below were also included in the majority opinion in the revised en banc decision.

Note 7: The pertinent wording [of s. 489] is "any thing that the [officer or person] believes on reasonable grounds" falls within paras. (a) to (c). Here, the most pertinent para. is (c) - anything that "will afford evidence in respect of an offence" against the *Criminal Code* or another federal statute.

Note 8: Respondent's factum, para. 55(c).