IS PASSWORD COMPULSION CONSTITUTIONAL IN CANADA? TWO VIEWS

By Robert Diab and Marshall Putnam

In January 2019 Downes J. of the Ontario Court of Justice issued a ruling on an unusual application in *R. v. Shergill*.[1] The Crown had sought a warrant to search a smartphone seized incident to arrest, along with an order to compel the accused to provide his password to police or unlock his phone. Contrary to the usual practice of seeking a warrant *ex parte*, the court heard submissions from both parties. Canada has no law explicitly authorizing a court to issue an order to compel a person to provide a password or a third party to assist with decryption.[2] Prior to *Shergill*, only a few courts had dealt with provisions that might be used to compel a password, broaching the issue of whether this would violate the right against self-incrimination or the right to silence.[3] But none of the cases had resulted in a ruling on the substance of the issue.[4]

The Crown in *Shergill* sought to make creative use of s. 487.02 of the *Criminal Code*, which allows a court to compel a party to assist in executing a warrant. The accused was charged with a series of sexual and child pornography offences involving his interactions with a 15-year-old girl. After police seized his phone on arrest, they obtained a warrant to search the data it contained, but the device was password protected. Justice Downes noted the "uncontradicted evidence" on the application that "police currently know of no technology which would allow them to access the contents without risking their destruction".[5] The Crown contended that its proposed use of s. 487.02 to compel a person to provide the pass-key was constitutional. Justice Downes disagreed, offering a compelling set of reasons on one side of a question many lawyers are wondering about: Could password compulsion be legal in Canada?

The question points, in turn, to a larger issue: the investigational impediment that encrypted data poses. How often police confront this issue is unclear.[6] Yet, over the last decade, data encryption has become pervasive in personal computing,[7] posing what can be, in a practical sense, an absolute barrier to lawful access.[8] For decades, privacy and security advocates have

debated whether mandating backdoors for law enforcement would compromise the benefits of encryption.[9] With that debate at an impasse, police and prosecutors have turned to password compulsion, giving rise to constitutional issues.

Case law and scholarship in Canada and the United States divide along clear lines.[10] We aim to briefly explain strong arguments for and against whether compelling a password or plaintext (the decrypted file or device) would violate the *Charter*.

Briefly, one side of the debate maintains that a law compelling accused persons to provide their password would violate the right against self-incrimination and the right to silence, because unlike a fingerprint, DNA or breath sample, a password is testimonial in nature. A compulsion order forces a person to "speak their mind" for the purpose of aiding the prosecution in producing a case to meet. Opponents argue that password compulsion is constitutional because disclosing a password is testimonial in only a perfunctory sense, and since accused persons do not create the plaintext by divulging their password, but only provide access to it, the plaintext is not derivative evidence that warrants immunity.

We note weaknesses in both arguments. The two contentious points are whether a password is testimonial in a sense that should engage the right against self-incrimination, and if so, how that right should be balanced against the state's interest in prosecuting cases on their merits.

THE FIRST VIEW: PASSWORD COMPLUSION IS UNCONSTITUTIONAL

The two main sources for this argument are law scholar N. Dalla Guarda's pioneering 2014 article in the *Criminal Law Quarterly*[11] and Downes J.'s reasons in *Shergill*. We draw here primarily on Downes J.'s reasons, given their application to particular facts.

The Crown in *Shergill* sought an order under s. 487.02 of the *Criminal Code* compelling the accused to unlock his phone. Section 487.02 states:

> If … a warrant is issued under this Act, the judge or justice who … issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant.

The court dismissed the application for an assistance order, holding that although the preconditions under s. 487.02 were met, granting the order would involve a breach of s. 7 of the *Charter*.[12]

Limiting its *Charter* submissions to the right against self-incrimination, the Crown argued that a password compulsion order under s. 487.02 would be *Charter*-compliant because it would only compel Mr. Shergill to give

access to material that police were authorized to examine; it would not compel him to create it.[13] The password itself had "no evidentiary value" and concerns about self-incrimination relating to his knowledge of the password itself could be addressed by granting immunity over this knowledge.[14]

The Crown drew an analogy between compelled passwords and compelled documents, citing the Ontario Court of Appeal's decision in *R. v. D'Amour*[15] for the legal proposition that "[d]ocuments that exist prior to, and independent of, any state compulsion do not … constitute evidence 'created' by the person required to produce those documents".[16] For this reason, as a general rule, compelling the production of documents does not engage the principle against self-incrimination.[17] The Crown also noted other powers permissible under the *Charter* that compel the accused to participate in gathering inculpatory evidence, including DNA warrants, breath samples and fingerprints.[18]

Justice Downes's decision calls into question each of the Crown's premises—namely, that a compelled password does not disclose the data itself, that the password itself is not incriminatory and that providing it facilitates rather than creates evidence. The issue requires the broader contextual analysis contemplated in *R. v. White*,[19] where Iacobucci J. held: "The principle against self-incrimination demands different things at different times, with the task in every case being to determine exactly what the principle demands, if anything, within the particular context at issue."[20] The Ontario Court of Appeal in *D'Amour* shed light on the principle's underlying rationale:

> [35] … Where the state alleges wrongdoing, it cannot force the target of that allegation to assist the state in proving the allegation. This rationale reflects the high premium placed on personal autonomy and individual privacy by the principles of fundamental justice. Those principles start from the premise that individuals are entitled to choose whether to cooperate with the state and, if they choose not to, to be left alone by the state. The rationale underlying the principle also reflects the hard learned lessons of history. Conscripted evidence is notoriously unreliable and the line between state compulsion and state abuse can be a fine one.

Drawing on these authorities, Downes J. held that "to focus exclusively on the incriminatory potential of the *password* neglects the significant incriminatory *effect* that revealing the password has on Mr. Shergill".[21]

In the court's view, without a compulsion order against Mr. Shergill, "the evidence would never come into the hands of the police".[22] Describing the data on the device as existing "prior to, and independent of, any state compulsion" was therefore "somewhat artificial".[23] The facts in *D'Amour* were different. The accused in *D'Amour* was charged with welfare fraud. The document at issue was a T4 slip that the accused was compelled to provide

prior to the criminal probe. Prosecutors could obtain it through other means.[24] By contrast, in *Shergill*, the assistance order, "[l]ooked at in any realistic and pragmatic sense", would procure for the Crown key evidence "brought into existence by the exercise of compulsion by the state".[25]

The argument that password compulsion violates the right against self-incrimination is founded on the Supreme Court's 1995 decision in *R. v. S. (R.J.)*.[26] Justice Iacobucci, for the majority, held that evidence is derivative "if it results, in fact, from a compelled disclosure".[27] The test is causal: "[o]nly evidence which comes to light as a result of a compelled disclosure" is derivative.[28] Where a causal connection is established, the evidence is obtained contrary to s. 7 of the *Charter* and "ought generally to be excluded under s. 7 of the *Charter* in the interests of trial fairness".[29] He added:

> Such evidence, although not created by the accused and thus not self-incriminatory by definition, is self-incriminatory nonetheless because the evidence could not otherwise have become part of the Crown's case. To this extent, the witness must be protected against assisting the Crown in creating a case to meet.[30]

Justice Iacobucci emphasized that in using the word "could" in this context, he was proposing "an inquiry into logical probabilities, not mere possibilities".[31] On this view, compelled access to the smartphone data in *Shergill* would be derivative because it is otherwise not discoverable and must therefore be protected by derivative use immunity to avoid violating s. 7.[32]

As a further rationale for opposing password compulsion, Downes J. pointed to the right to silence, "the more significant principle of fundamental justice at stake".[33] In *R. v. Hebert*,[34] McLachlin J., as she then was, framed the right expansively:

> [I]f the *Charter* guarantees against self-incrimination at trial are to be given their full effect, an effective right of choice as to whether to make a statement must exist at the pre-trial stage. … the right to silence of a detained person under s. 7 of the *Charter* must be broad enough to accord to the detained person a free choice on the matter of whether to speak to the authorities or to remain silent.[35]

For Downes J., it was the "testimonial nature of the compulsion contemplated by the assistance order" that distinguished it from orders relating to physical forms of evidence such as DNA or breath samples.[36] The order would, in effect, require Mr. Shergill "to 'speak his mind' to the police", providing help "through an utterance conveying a thought in his head".[37] Compelling a person to this degree seemed, to Downes J., to be altogether anomalous: "To my knowledge, there are no other provisions related to criminal prosecutions in Canada which require an accused to provide utterances fundamentally designed to assist in the obtaining of evidence against him or her."[38]

Justice Downes concluded by considering the Supreme Court's holding in *White* that "[i]n some contexts, the factors that favour the importance of the search for truth will outweigh the factors that favour protecting the individual against undue compulsion by the state".[39] Police face a serious challenge with encryption, and other approaches may be warranted. But as Guarda had done before him, Downes J. concluded that the weight of authority strongly suggested that a password compulsion order could not issue without "fundamentally breaching Mr. Shergill's s. 7 liberty interests".[40]

Problems with This Argument

We see two shortcomings. First, Downes J. construed the act of providing a password as a form of testimony but offered little argument for why it must be seen as such. His construal of passwords as a form of testimony permitted his inference that an order would be self-incriminating if it were to yield inculpatory evidence—if it has a certain positive evidentiary effect for the prosecution. But the effect does not determine whether a password is essentially "testimonial in nature".[41]

Second, Downes J. did not clearly identify the nature of the state's interest in compelling a password. Does it merely help the state acquire so-called documentary evidence, or does it prevent investigations from stalling? Much turns on the difference. The Supreme Court authority suggests that a serious violation of s. 7 of the *Charter* cannot be justified for mere expedience.[42] Guarda and other pro-privacy advocates doubt encryption poses an insurmountable hurdle to prosecutions.[43] There are other avenues for police to obtain evidence in cases involving computer-related crimes, such as powers for covert surveillance, capturing passwords at encryption endpoints through surreptitious but lawful means, or data from a growing abundance of other sources.[44] Yet, as one scholar notes, a substitute for evidence lost to police through encryption cannot always be found through other means.[45]

In these cases, precluding password compulsion allows s. 7 *Charter* rights to act as a trump card, suggesting that the state interest bears little or no weight. In relatively minor cases, this may be reasonable, but in more serious cases (e.g., murder, sexual assault), it may not. Courts should be equipped to conduct a more detailed inquiry, not unlike the kind we conduct under s. 24(2) of the *Charter*.[46] An analogous balancing test might be fashioned under s. 7 leading to a compulsion order in more serious cases where the state establishes no other means of obtaining the evidence.

THE SECOND VIEW: PASSWORD COMPULSION IS CONSTITUTIONAL

Steven Penney and Dylan Gibbs's 2017 article in the *McGill Law Journal* is

the latest and most extensive scholarly treatment of password compulsion in Canada.[47] The authors anticipate the outcome in *Shergill* by noting the possible use of s. 487.02 for this purpose but doubting that courts would find it constitutional.[48] Yet the thrust of their paper argues that a law can be crafted that strikes the right balance between state and individual interests, and that Canada should follow recent British and Australian examples.[49]

Penney and Gibbs see an important distinction in post-*Charter* case law between linguistic and non-linguistic forms of compulsion. The Supreme Court has considered the latter class—fingerprints, breath samples and DNA samples—not through the lens of self-incrimination but instead as forms of search under s. 8.[50]

The authors see password compulsion as sharing aspects of linguistic and non-linguistic compulsion but assert that "the encryption key itself should be viewed as non-linguistic compulsion".[51] A password communicates information "in a manner categorically different from the kinds of linguistic acts traditionally enjoying self-incrimination protection".[52] Passwords serve a "purely mechanistic purpose", are not expressive and convey nothing about the "material world or the user's experience of it".[53]

The authors derive this distinction from case law on free expression under s. 2(b) of the *Charter*, where courts distinguish expressive from purely functional forms of speech (e.g., voice commands to adjust a car's speed). The latter forms do not merit protection because they have no "expressive character" or "outcome".[54] Impliedly, what is not worth protecting as expression is not worth protecting as self-incrimination.[55]

Passwords bear further similarity to other non-linguistic (e.g., DNA, fingerprints) forms of compulsion. They may originate in the mind, but they have "an independent, material existence analogous to a physical key".[56]

Earlier *Charter* jurisprudence on compelled evidence offers a roadmap for how password compulsion could be constitutional. The authors see a close analogy in *R. v. Orbanski*,[57] a case where the Supreme Court upheld the constitutionality of roadside sobriety tests. It held that demanding a person to submit to a physical sobriety test would be self-incriminating if the test result were admitted as evidence of impairment, but not if used only as a ground for demanding a breath sample.[58]

The authors see the logic in *Orbanski* mapping closely onto password compulsion. Sobriety tests compel a suspect's participation to create "communicative evidence" that may be self-incriminating: "bodily movements = probably drunk", but using this evidence to make physical evidence available (the bodily samples or breath samples to show impairment) is not self-incriminating.[59] Similarly, a decryption order compels a person to create

new communicative evidence that may be self-incriminating (i.e., the ability to decrypt shows connection to the data), but the use of that evidence to make pre-existing physical evidence available (plaintext) to prove the offence is not.

The same logic extends to an order to provide the plaintext itself, an alternative that avoids the "plainly linguistic and communicative" act of providing a key.[60] An order for plaintext has the merit of not requiring a person to disclose anything that exists "independent of the compulsion, beyond the implied statement that they can decrypt the data".[61] Thus, in contrast to Downes J.'s view in *Shergill*, Penney and Gibbs do not conceive an order for either plaintext or a password as a means of forcing the accused to assist in *creating* evidence. The difference matters, given the Supreme Court's holding in *British Columbia Securities Commission v. Branch*[62] (also cited in *Shergill*) that the principle against self-incrimination applies only to material "brought into existence by the exercise of compulsion by the state".[63]

In summary, by framing a password as non-linguistic and the plaintext as pre-existing and not created, Penney and Gibbs circumvent the issue of discoverability noted in *Shergill*. Penney and Gibbs's analysis omits the argument that without the suspect or accused providing a password, the plaintext would likely never be found.

In the authors' view, applying the test for compelled evidence set out in *R. v. Fitzpatrick*,[64] either form of compulsion, key or plaintext, would withstand a s. 7 challenge. Neither password nor plaintext compulsion violates the purposes underlying the protection against self-incrimination: avoiding unreliable confessions or abuses of state power. A person either provides the correct password or they do not.[65] And although state abuse may arise through excessive force or inhumane tactics, "a statutory obligation to decrypt is likely to diminish this risk, not enhance it".[66] Courts could also grant derivative use immunity for the accused's knowledge of the password, but not the plaintext itself, since it pre-exists the compulsion and "therefore cannot be said to derive from it".[67]

The Supreme Court has held "outright" prohibitions on compulsion are justified only "when the state's predominant purpose is to obtain self-incriminating evidence, rather than some other legitimate public purpose".[68] Penney and Gibbs suggest that the state has a legitimate interest in compelling a password or plaintext: "helping police render intelligible information that they are legally entitled to possess".[69] Prohibiting compulsion "would simply serve as a shield for wrongdoing".[70]

Viewing password compulsion as a form of non-linguistic compulsion to be assessed under s. 8, the authors propose a law requiring police to obtain

a compulsion warrant on reasonable suspicion that the user has "the capacity to access encrypted data that police are lawfully entitled to possess".[71]

Problems with This Argument

The core of Penney and Gibbs's argument is the analogy they draw to *Orbanski*. Is an order to compel a password like an order to perform a sobriety test? The two are similar in that neither the sobriety test nor the password is used as evidence of the offence (impairment, possession of illicit data). But they differ in one crucial respect: in many if not most cases, a sobriety test offers one among several means of gathering grounds for a breath demand (disheveled clothing, odours, a driving pattern), and for this reason the test is seldom used. By contrast, in a case like *Shergill*, a password provides the only means of accessing the plaintext. A sobriety test makes prosecution easier; a password makes it possible.

Penney and Gibbs might concede this point but argue that passwords are still not testimony in a meaningful sense, exist independently and are thus no different from a fingerprint or DNA sample. But here too, the analogy breaks down. The alphanumeric password may exist independently of being uttered and is therefore not "created" by being disclosed. But a password held only in a person's mind cannot be yielded without an act of speech (nor a plaintext disclosed) or forcing a person to act on their internal knowledge. This involves a deeper form of compulsion than taking a hair sample or a fingerprint. Police can use force in the latter case, but one might still be defiant (unpleasant though it may be). The distinction is not absolute. In both cases, one's freedom to choose is seriously affected. But with compelled decryption, the state power contemplates a person's complete *internal* conscription.

CONCLUSION

With time, technology may render this issue moot. For the foreseeable future, forms of encryption that police find practically impregnable are likely to persist. Courts and lawmakers will continue to grapple with a series of crucial questions: Should we consider divulging a password a non-testimonial or linguistic act? If we compel a password to access evidence we would not otherwise obtain, do we conscript a person in *creating* the evidence against them? And what is the state's purpose in compelling a password or plaintext: merely to access evidence when lawfully entitled, or to conscript the accused in producing a case to meet? There are no clear answers. The legality of password compulsion thus remains a code we have yet to crack.

ENDNOTES

1. 2019 ONCJ 54 [*Shergill*].
2. See Government of Canada, Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016* (Ottawa: Her Majesty the Queen in Right of Canada, 2016) at 61, online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx>.
3. In *R v Hebert*, [1990] 2 SCR 151 [*Hebert*], the Supreme Court of Canada recognized the right to silence as a "principle of fundamental justice" protected under s 7 of the *Charter*. The right against self-incrimination for testimony given in proceedings is protected under ss 11(c) and 13 of the *Charter*, and the Supreme Court has held that s 7 protects against self-incrimination in other contexts. See *R v White*, [1999] 2 SCR 417 [*White*].
4. The earlier decisions broaching the issue include *R c Boudreau-Fontaine*, 2010 QCCA 1108 and *R v Talbot*, 2017 ONCJ 814.
5. *Shergill*, *supra* note 1 at para 1.
6. See e.g. Devlin Barrett, "FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public", *Washington Post* (22 May 2018), online: <www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html> (noting that the nearly 7,800 estimate of the number of devices the FBI could not access in the course of investigations in 2017 had been incorrect and the number is probably between 1,000 and 2,000).
7. We have in mind here the use of encryption in Apple's iOS, Android OS and in services such as iMessage, Gmail and WhatsApp.
8. See the discussion of the "strength of a cryptographic system" in Lex Gill, Tamir Israel & Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide* (Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2018) at 3, online: <citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>.
9. See e.g. Harold Abelson et al, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report (Cambridge, Mass: Massachusetts Institute of Technology, 2015).
10. On Canadian law, see N Dalla Guarda, "Digital Encryption and the Freedom from Self-Incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" (2014) 61:1 Crim LQ 119; Steven Penney & Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*" (2017) 63:2 McGill LJ 201. On US law, see Aloni Cohen & Sunoo Park, "Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries" (2018) 32:1 Harv J Law & Tech 170; Orin S Kerr, "Compelled Decryption and the Privilege Against Self-Incrimination" (2019) 97:4 Tex L Rev 767.
11. *Supra* note 10.
12. *Shergill*, *supra* note 1 at paras 9–10.
13. *Ibid* at para 3.
14. *Ibid* at para 18. See also s 487.0196 of the *Criminal Code*.
15. 2002 CanLII 45015 (Ont CA) [*D'Amour*].
16. *Ibid* at para 37.
17. *Ibid*. Justice Doherty wrote: "With certain narrow exceptions, neither the compelled production of such documents, nor the subsequent use in a criminal proceeding of such documents, attracts the protection of the principle against self-incrimination".
18. *Shergill*, *supra* note 1 at para 24.
19. *Supra* note 3.
20. *Ibid* at para 45, quoted in *Shergill*, *supra* note 1 at para 25.
21. *Shergill*, *supra* note 1 at para 19 [emphasis in original].
22. *Ibid* at para 31.
23. *Ibid*.
24. See *D'Amour*, *supra* note 15 at para 42.
25. *Shergill*, *supra* note 1 at para 31, citing *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3 at para 43 [*BC Securities*].
26. [1995] 1 SCR 451 [*S (RJ)*].
27. *Ibid* at 546.
28. *Ibid*, cited in *Shergill*, *supra* note 1 at para 32.
29. *S(RJ)*, *supra* note 26 at 561, cited in *Shergill*, *supra* note 1 at para 35.
30. *S(RJ)*, *supra* note 26 at 561 [emphasis in original], cited in *Shergill*, *supra* note 1 at para 35.
31. *S(RJ)*, *supra* note 26 at 562, cited in *Shergill*, *supra* note 1 at para 36.
32. *Shergill*, *supra* note 1 at para 38.
33. *Ibid* at para 21.
34. *Supra* note 3.
35. *Ibid* at 178, quoted in *Shergill*, *supra* note 1 at para 21.
36. *Shergill*, *supra* note 1 at para 41.
37. *Ibid*.
38. *Ibid*.
39. *White*, *supra* note 3 at para 48, quoted in *Shergill*, *supra* note 1 at para 44.
40. *Shergill*, *supra* note 1 at para 51. See also Guarda, *supra* note 10 at 137 ("if the Canadian state were to carve out an exception to self-incrimination law for encrypted data, it would entail crossing a centuries-old line which has hitherto ensured that individuals would never be coerced into contributing to their own prosecution … . Crossing that line … is not only normatively undesirable, but it is also improbable given the pedigree of the constitutional rights which would be sacrificed" [footnote omitted]).
41. Guarda, *supra* note 10 does the same. See the portion of his article titled "Framing Passwords as Testimonial" (133–35), setting out consequences that flow from construing password compulsion as compelled testimony, rather than reasons why it *is* a form of testimony.

42. In *Re BC Motor Vehicle Act*, [1985] 2 SCR 486, Lamer J, as he then was, wrote for the majority: "Section 1 may, for reasons of administrative expediency, successfully come to the rescue of an otherwise violation of s. 7, but only in cases arising out of exceptional conditions, such as natural disasters, the outbreak of war, epidemics, and the like" (para 85).
43. See e.g. Gill, Israel & Parsons, *supra* note 8, Part 5 ("Encryption Is Not an Insurmountable Barrier").
44. See *ibid*. See also Guarda, *supra* note 10 at 140–42.
45. See Justin Hurwitz, "Encryption Congress Mod (Apple + CALEA)" (2017) 30:2 Harv J Law & Tech 355 at 401.
46. See *R v Grant*, 2009 SCC 32.
47. Penney & Gibbs, *supra* note 10.
48. *Ibid* at 209, n 32.
49. In the United Kingdom: *Regulation of Investigatory Powers Act* 2000 (UK), c 23, ss 49–56. In Australia: *Crimes Act 1914* (Cth), s 3LA.
50. See Penney & Gibbs, *supra* note 10 at 232, n 128 and accompanying text, citing as examples *R v Beare; R v Higgins*, [1988] 2 SCR 387 (on mandatory fingerprinting); *R v Thomsen*, [1988] 1 SCR 640 (on bodily samples in impaired driving cases); and *R v Bernshaw*, [1995] 1 SCR 254 (on breath samples in impaired driving cases)—none of which mentions self-incrimination.
51. Penney & Gibbs, *supra* note 10 at 233.
52. *Ibid*.
53. *Ibid*.
54. *Ibid* at 227.
55. *Ibid*, citing *Irwin Toy Ltd v Quebec (Attorney General)*, [1989] 1 SCR 927 at 968–71.
56. Penney & Gibbs, *supra* note 10 at 234.
57. *R v Orbanski; R v Elias*, 2005 SCC 37 [*Orbanski*].
58. Penney & Gibbs, *supra* note 10 at 234.
59. *Ibid*.
60. *Ibid*.
61. *Ibid* at 234–35 [footnote omitted].
62. *Supra* note 25.
63. Penney & Gibbs, *supra* note 10 at 235, quoting *BC Securities*, *supra* note 25 at para 43.
64. [1995] 4 SCR 154.
65. Penney & Gibbs, *supra* note 10 at 238. The authors acknowledge the possibility of a conviction for failing to comply with a decryption order resulting from a simple failure to remember a password. To remove this prospect, they propose a strong *mens rea* requirement: "knowingly" or "willfully" refusing to comply. See *ibid* at 237, n 148.
66. *Ibid* at 238.
67. *Ibid* at 239, n 162.
68. *Ibid* at 240 [footnote omitted].
70. *Ibid*.
71. *Ibid* at 243.

Leanne Christie, detail of *Changing Cordova*, oil on canvas, 60" x 72"
Available through Art Rental & Sales at the Vancouver Art Gallery, www.artrentalandsales.com