KORNFELD LLP

1100 ONE BENTALL CENTRE
505 BURRARD STREET, BOX 11
VANCOUVER, B.C., CANADA V7X 1M5
T: 604.331.8300 F: 604.683.0570
WWW.KORNFELDLLP.COM

Shafik Bhalloo
sbhalloo@kornfeldllp.com
d: 604-331-8308

Supreme Court rules that employees have a reasonable expectation of privacy in the workplace

In *R. v. Cole*[1], a high school teacher, who also worked with the school's IT department in supervising computer use by students and staff, had authority to remotely access the data stored on student computers connected to the school network and accessed a student's email account. The teacher found nude photographs of another student and copied them onto the hard drive of his school-issued laptop. Under the school's Acceptable Use Agreement ("UA"), the teacher was allowed to use his work-issued laptop for both work and personal purposes. When a technician employed by the school, while performing regular maintenance work on the teacher's laptop, discovered a hidden folder on the teacher's laptop containing the said photographs, he notified the school's principal. Pursuant to the latter's instructions, the technician copied the pictures to a compact disc. The principal, subsequently, seized the laptop and, thereafter, the technician copied, on a second compact disc, temporary internet files from the laptop. The laptop was then turned over to the police, together with the two discs. The police, without obtaining a search warrant in advance, examined the contents of the laptop and the two discs and created a mirror image of the laptop's hard drive. The teacher was later charged with possession of child pornography.

At trial, the teacher applied and was successful under section 8 and subsection 24(2) of the *Canadian Charter of Rights and Freedoms* to have the evidence against him excluded on the basis that it was obtained in a manner violating his constitutional rights under the *Charter*. On appeal by the Crown, the Ontario High Court of Justice reversed the lower court's decision, finding that the trial judge erred in law in concluding that Mr. Cole had an objectively reasonable subjective expectation of privacy stating that the judge erroneously ignored the following contextual factors:

- The teacher's acceptance of the employer's UA as terms of his employment, which afforded him knowledge that the data and information on the computer and drives assigned to him by the employer were not private;
- The teacher also worked with the school's IT department staff to supervise and monitor both the computer use by students and staff of the high school and the overall integrity of the school's network, and, in this supervisory capacity, the teacher had domain-wide privileges which demonstrated to him that the data on his computer drives was accessible by employer representatives such as himself;
- In light of the first two points above, indicators such as the teacher's password and his exclusive possession of the laptop as part of his employment were not privacy indicators;
- The teacher's knowledge that the hardware and software in and connected to the laptop belonged to the employer.

On appeal by the teacher, the Court of Appeal of Ontario set aside the latter decision in part holding that the disc containing the temporary internet files, the laptop and the mirror image of its hard drive should be excluded. The Court of Appeal reasoned as follows:

> [76] … the fact that the discs and laptop in this case had been lawfully seized by the principal and the school board and delivered to the police does not affect the continuing privacy expectations of the appellant. Police are not relieved from the stringent standard of obtaining judicial authorization to conduct a search or seizure based on reasonable and probable grounds, simply because they are provided with evidence in circumstances where the accused's *Charter* rights were either not engaged or were not infringed in the initial gathering of that evidence….
>
> [77] …The appellant's privacy interest with respect to his laptop continued throughout its transfer to police, notwithstanding that it was the property of the school board, and already lawfully seized by them. Personal information was also stored on the laptop.
>
> The police conducted a search and seizure of the laptop and seized the mirror image of the hard drive, capturing every piece of personal information the appellant may have stored on it, including the photographs of his wife, without a warrant.
>
> [78] The appellant also had a privacy interest in his personal internet browsing history and what it revealed about his personal predilections and choices. In *R. v. Morelli*, 2010 SCC 8 (CanLII), [2010] 1 S.C.R. 253, at para. 3, the Supreme Court referred to this as 'the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet'. Because the appellant had a continuing privacy interest in this information, the transfer of the disc with the temporary internet files to the police was a 'seizure' within the meaning of s. 8 of the *Charter*.
>
> [79] The police search of the laptop and the disc with the temporary internet files is therefore *prima facie* unreasonable. The onus shifts to the Crown to establish that this warrantless search by police was nonetheless reasonable. There were no exigent circumstances. Both the school environment and the evidence were secure; the teacher was suspended and the police were in possession of the discs and the laptop. The school board had no authority to consent to the search. This warrantless search was not reasonable. Therefore, the police violated the appellant's s. 8 rights when they searched the laptop and the disc with the temporary internet files.

However, the Court of Appeal viewed the disc containing images of the student differently, stating:

> Given that the photographs were taken from the school's network, using the school's computer and were the subject of the privacy interest of a student, the appellant had no personal privacy interest in the data. The photographs were found by the technician in plain view, while engaged in permissible access. They were lawfully seized by the principal and transferred to police. As the functional equivalent of photographs in an envelope, the police did not need to conduct a further search of this evidence. Because the appellant had no privacy interest in the photographs themselves (as opposed to the presence of those photographs in the laptop), the delivery of the disc to police was not a seizure.

On Appeal by the Crown, the Supreme Court of Canada, while agreeing with the Court of Appeal that the teacher had a reasonable expectation of privacy in the circumstances and the police infringed the teacher's privacy protected under section 8 of the *Charter*, allowed the appeal and set aside the decision of the Court of Appeal. In arriving at this conclusion, Mr. Justice Fish, writing for the majority of the Supreme Court, delineated the following instructive principles:

- Whether at home or in the workplace, computers are reasonably used for personal purpose and contain information that is meaningful, intimate and touching on the user's biographical core;
- The user may reasonably expect privacy in the information contained on their computer particularly where personal use is permitted or reasonably expected;
- While ownership of the computer and workplace policies are relevant considerations, neither is determinative of a person's reasonable expectation of privacy;

- The totality of all the circumstances will need to be considered to determine whether privacy is a reasonable expectation in any particular case;
- Workplace policies and practices may diminish an individual's expectation of privacy in a work computer; however they may not in themselves remove the expectation entirely;
- A reasonable, though diminished expectation of privacy, is nonetheless a reasonable expectation of privacy, protected by s. 8 of the Charter and subject only to state intrusion under the authority of a reasonable law.

Applying the above principles to the facts in this case, Fish J. stated the operational realities of the teacher's workplace consisted of factors that pulled in competing directions. In particular, Fish J. noted that while the written policy, and actual practice at work, permitted the teacher to use his work-issued laptop for personal purpose, the policy and technological reality deprived him of exclusive control and access to the personal information he recorded on the laptop. More particularly, Fish J. noted that the written policy of the school, of which the teacher was reminded by the principal annually, provided that the data and messages generated on or handled by the employer's equipment was owned by the employer and he was aware that the contents of his hard drive were available to all other users and technicians with domain administration right. On the totality of the circumstances, Fish J. concluded that the teacher had a reasonable subjective expectation of privacy in his internet browsing history and the informational content of his work-issued laptop; it contained information that was meaningful, intimate and touching on his biographical core.

Having said this, however, the Supreme Court did not find the school to have acted unreasonably or in breach of s. 8 of the *Charter* when its technician inspected the teacher's laptop in context of routine inspection or when the school subsequently seized the laptop at the instruction of the principal because the school's principal had a statutory duty to maintain a safe school environment. However, the school's lawful authority did not afford the police lawful authority to conduct a warrantless search and seizure of the computer material and examine its contents, according to the Supreme Court. In particular, Fish J. reasoned:

> [67] In taking possession of the computer material and examining its contents, the police acted independently of the school board (*R. v. Colarusso*, 1994 CanLII 134 (SCC), [1994] 1 S.C.R. 20, at pp. 58-60). The fact that the school board had acquired lawful possession of the laptop *for its own administrative purposes* did not vest in the police a delegated or derivative power to appropriate and search the computer *for the purposes of a criminal investigation*.
>
> …
>
> [73] The school board was, of course, legally entitled to inform the police of its discovery of contraband on the laptop. This would doubtless have permitted the police to obtain a warrant to search the computer for the contraband. But receipt of the computer from the school board did not afford the police *warrantless access* to the personal information contained within it. This information remained subject, at all relevant times, to Mr. Cole's reasonable and *subsisting* expectation of privacy.

Having found that the police breached the teacher's privacy rights under section 8 of the *Charter*, Fish J. embarked on an inquiry under s. 24(2) of the *Charter*, namely, whether the unconstitutionally-obtained evidence by the police should be excluded. Here, Fish J. considered a three-part balancing test set out in the Supreme Court's decision in *R. v. Grant*[2]. In particular, Fish J. considered (i) the seriousness of the *Charter*-infringing conduct of the police; (ii) the impact of the breach on the *Charter*-protected interest of the teacher; and (iii) the society's interest in the adjudication of the case on its merits. In setting aside the decision of the Court of

Appeal and allowing the unconstitutionally-obtained evidence, Fish J. stated with respect to the first part of the *Grant* test:

> [84] Regarding the seriousness of the *Charter*-infringing conduct, the courts below focused on the actions of Detective Constable Timothy Burtt, the officer who took possession of the computer material, who searched the discs, and who sent the laptop away for forensic examination. The trial judge concluded that this officer's actions were 'egregious' (para. 26), and the Court of Appeal considered his conduct serious enough to favour exclusion.
>
> [85] I am unable to share either conclusion.
>
> [86] The police officer did not knowingly or deliberately disregard the warrant requirement. As events were unfolding in this case, the law governing privacy expectations in work computers was still unsettled. Without the guidance of appellate case law, D.C. Burtt believed, erroneously but understandably, that he had the power to search without a warrant.
>
> [87] He did not act negligently or in bad faith. Nor does his conduct evidence insensitivity to *Charter* values, or an unacceptable ignorance of Mr. Cole's rights under the *Charter*. The officer did not rely exclusively, as the courts below suggested, on his mistaken belief that the ownership of the laptop was necessarily determinative. While this was an important factor underlying his decision not to obtain a search warrant, the officer also turned his mind to whether Mr. Cole had an expectation of privacy in the laptop (p. 130). He was alert to the possibility that the hard drive contained private or privileged material (pp. 130-31 and 164). And he testified that he intended to respect Mr. Cole's privacy interest in this regard (p. 131).
>
> …
>
> [89] …Where a police officer could have acted constitutionally but did not, this might indicate that the officer adopted a casual attitude toward — or, still worse, deliberately flouted — the individual's *Charter* rights (*Buhay*, at paras. 63-64). But that is not this case: The officer, as mentioned earlier, appears to have sincerely, though erroneously, considered Mr. Cole's *Charter* interests.
>
> [90] Accordingly, in my view, the trial judge's finding of 'egregious' conduct was tainted by clear and determinative error (*Côté*, at para. 51). On the undisputed evidence, the conduct of the officer was simply not an egregious breach of the *Charter*. As earlier seen, the officer did attach great importance to the school board's ownership of the laptop, but not to the exclusion of other considerations. He did not 'confuse ownership of hardware with privacy in the contents of software' (trial reasons, para. 29).

With respect to the second part of the *Grant* test, Fish J. stated:

> [91] Turning then to the impact of the breach on Mr. Cole's *Charter*-protected interests, the question relates to 'the extent to which the breach actually undermined the interests protected by the right infringed' (*Grant*, at para. 76). In the context of a s. 8 breach, as here, the focus is on the magnitude or intensity of the individual's reasonable expectation of privacy, and on whether the search demeaned his or her dignity (*R. v. Belnavis*, 1997 CanLII 320 (SCC), [1997] 3 S.C.R. 341, at para. 40; *Grant*, at para. 78).
>
> [92] In his s. 24(2)analysis, the trial judge neglected entirely to consider the diminished nature of Mr. Cole's reasonable expectation of privacy. Likewise, the Court of Appeal overlooked the fact that the operational realities of Mr. Cole's workplace attenuated the effect of the breach on his *Charter*-protected interests.
>
> [93] Moreover, the courts below failed to consider the impact of the 'discoverability' of the computer evidence on the second *Grant* inquiry. As earlier noted, the officer had reasonable and probable grounds to obtain a warrant. Had he complied with the applicable constitutional requirements, the evidence would necessarily have been discovered. This further attenuated the impact of the breach on Mr. Cole's *Charter*-protected interests (*Côté*, at para. 72).

Finally, with respect to the third part of the *Grant* test, Fish J. stated:

> Finally, I turn to the third *Grant* inquiry: society's interest in an adjudication on the merits. The question is 'whether the truth-seeking function of the criminal trial process would be better served by admission of the evidence, or by its exclusion' (*Grant*, at para. 79).

> [95] Not unlike the the considerations under the first and second inquiries, the considerations under this third inquiry must not be permitted to overwhelm the s. 24(2) analysis (*Côté*, at para. 48; *R. v. Harrison*, 2009 SCC 34 (CanLII), 2009 SCC 34, [2009] 2 S.C.R. 494, at para. 40). They are nonetheless entitled to appropriate weight and, in the circumstances of this case, they clearly weigh against exclusion of the evidence.
>
> [96] The laptop, the mirror image of its hard drive, and the disc containing Mr. Cole's temporary Internet files are all highly reliable and probative physical evidence. And while excluding it would not "gut" the prosecution entirely, I accept the Crown's submission that the forensic examination of the laptop, at least, is "critical": the metadata on the laptop may allow the Crown to establish, for example, when the photographs were downloaded and whether they have ever been accessed.
>
> [97] In sum, the admission of the evidence would not bring the administration of justice into disrepute. The breach was not high on the scale of seriousness, and its impact was attenuated by both the diminished privacy interest and the discoverability of the evidence. The exclusion of the material would, however, have a marked negative impact on the truth-seeking function of the criminal trial process.

For the above reasons, Fish J. did not exclude the evidence unlawfully obtained by the police.

While the case is a criminal one and engages an individual's privacy rights under s. 8 of the *Charter* since it involves state (police) intrusion of an individual's privacy rights, the privacy principles articulated by Fish J. will undoubtedly be considered by courts in future employment law cases and employers should be mindful of those principles in structuring their relationship with their employees.

It is recommended that employers should implement clear policies that define, in unequivocal terms, the employer's expectations surrounding workplace computer use, including smartphone use, if employers provide such equipment to employees in an employment context. Although Fish J., in *R. v. Cole,* stated that workplace policies are not determinative of a person's reasonable expectation of privacy, if properly drafted a workplace policy combined with consistent employer actions in the workplace, may diminish, objectively, the employee's reasonable expectation of privacy. For example, where both the employer's workplace policy and the employer's actions in the workplace are consistent in prohibiting any personal use by employees of employer-issued computers or smartphones and where the employee has acknowledge receipt of employer's policy that provides that any data sent, stored or received using the employer's computer or smartphone is the property of the employer and the employer reserves the right to perform random checks or audits of the employee's computer or smartphone use, the employee may be hard pressed to argue that he or she has a reasonable expectation of privacy.

Shafik Bhalloo has been a partner of Kornfeld LLP since 2000. His practice is focused on labour and employment law, and on commercial and civil litigation. He is also an Adjudicator on the Employment Standards Tribunal and an Adjunct Professor in the Faculty of Business Administration at Simon Fraser University.
sbhalloo@kornfeldllp.com
http://www.kornfeldllp.com/vcards/sbhalloo.vcf
604.331.8308

---

[1] 2012 SCC 53

[2] 2009 SCC 32