Conference report: Privacy Laws and Effective Workplace Investigations

The privacy implications of workplace investigations was the theme of a Vancouver conference held by Insight Information, April 23-24th. The conference examined a broad range of issues, from means to make organisations privacy compliant, to privacy rights and sexual harassment in the workplace. Over the next four pages, **Eugene Oscapella** highlights some of the key issues addressed at the conference.

Building a culture of respect for privacy among employees

How can organisations encourage employees to share their vision of a privacy-compliant workplace?

Former British Columbia Information and Privacy Commissioner Dr David Flaherty, now a privacy consultant, stated his concern about the extent of unauthorised access to personal information occurring in public institutions by individuals who do not have a "right to know". This situation was worsening because of the increasing number of automated data storage systems held by groups such as the police, and in institutions such as hospitals.

The inspiration for such collection, argued Flaherty, may simply be the power that flows from holding information. He cited as one example a Canadian police officer who was opposed to abortion and who had used his police computer to obtain information about individuals attending an abortion clinic from the licence plates on their cars parked at the clinic.

In an environment of unauthorised access, claimed Flaherty, it is very difficult to create a culture of respect for privacy. Still, there are ways to succeed.

Introducing a culture of privacy is like introducing any other form of "cultural" change to an organisation. The same kinds of skills that are brought to bear on any other management issue must be used to introduce a culture of privacy. It requires consciousness-raising "from the top down and bottom up". Everyone in management must be made to understand privacy issues. Human resources professionals, he suggested, generally have a very good understanding of privacy issues; many fair information practices are likely already ingrained with them. The challenge is to expand this knowledge throughout the organisation.

> an organisation's privacy culture requires maintenance and continuous improvements through audits and onsite visits

Flaherty identified a series of prerequisites for creating a culture of privacy. First, privacy policies must be known and understood. Procedures to complement those policies must also be established. Furthermore, the more "privacy intensive" the nature of an organisation's work (a hospital vs a hardware store, for example), the more seriously it must take privacy.

Frequently Asked Questions (FAQs), he stated, are an effective way to help employees and customers understand the implications of privacy. For example, customers need to be told what information is collected about them and what is done with it. Often, these FAQs can be modelled on those from other sites.

Creating an awareness of the importance of privacy cannot be a one-time activity. Privacy team members must "have their noses to the ground," said Flaherty. "They have to mix with the troops." Organisational intranets can also be used to maintain awareness and inform employees of developments and issues.

Training, he added, is the key to effective implementation of a privacy culture. It may be best to have human resources training experts identify how to communicate information most effectively, since the type and amount of training required will vary among employees. Training can be accomplished through online programmes, intranet communications and by adding privacy modules to existing organisational training programmes. Once training begins, it will also be necessary to identify the individual or individuals responsible for responding to questions about privacy issues. The questions fielded by such individuals will help identify the issues that need to be addressed in the organisation's privacy FAQs.

Establishing accountability is also an essential building block for a privacy culture. Organisational management teams were initially sceptical of the concept of the Chief Privacy Officer (CPO). Now, however, more are convinced of the need. The CPO should report directly to senior management - preferably the Chief Information Officer (CIO) or CEO.

Flaherty also recommended building a privacy "team" to address ongoing privacy issues. Representatives from legal affairs, human resources, communications, IT, marketing, the CIO, and senior management should meet periodically to try and solve problems internally. In addition, a crisis management approach must be put in place in advance of any possible privacy crisis. "How will the organisation respond when a reporter calls to ask what happened to records that fell off the back of a truck?" asked Flaherty.

The CPO can be particularly useful in establishing an internal process to resolve privacy issues, thereby avoiding customers or employees appealing directly to the "privacy police" - privacy or data protection authorities. However, the CPO cannot be expected to resolve all privacy issues. It may be necessary to devolve responsibility to others for certain decisions relating to privacy. For example, the level of privacy risks that a company should tolerate may be a decision to be made by the CEO, not the CPO.

Even once established, an organisation's privacy culture requires maintenance and continuous improvements through audits and onsite visits, says Flaherty. The organisation must ensure that privacy rules and procedures work in practice. Audit trails are an obvious tool. CPOs could even consider proactive ongoing auditing. Furthermore, technology can increasingly be used to build in "privacy by design".

Privacy officers must keep their eyes open. What they see in onsite visits - for example, a fax machine in a public area, with sensitive documents thrown into a nearby trash bin - may help them act in time to avoid a privacy crisis.

Using computer forensics to combat e-theft

According to consultancy firm KPMG, hi-tech information thefts carried out by employees are requiring businesses to adopt an increasingly sophisticated approach to investigations.

Owen Key and Brent Homberger, both of KPMG Forensic Technology Services, explained how dishonest employees sometimes use highly sophisticated programs to steal corporate information. Hi-tech thefts from corporations, they noted, are mostly internal, involving current or past employees, contractors, cleaning staff, or the relatives of any of these. Their presentation described the role of computer forensics in obtaining and preserving evidence of improper activities.

Computer forensics involves preserving electronic evidence in its original state to enable others to restore the information and obtain the same results, should this be required. In short, computer forensics take a snapshot (not a copy) at a given point of time of a piece of information that may be stored electronically. Simply copying files from an employee's computer is not a good forensic technique, since it changes the times associated with the documents. Computer forensics involves backing up information in a form that does not change the media and the associated times. As with other forms of evidence in legal proceedings, forensic investigators are seeking to prove the "chain of evidence" and that the evidence is authentic.

Key and Homberger explained that hitting the "delete" button does not mean that the information disappears from the computer's hard drive. This action merely tells the computer that these files can be overwritten, but the files may nonetheless remain partially or wholly intact on the computer for years. Nor does formatting a hard drive mean that information is gone from the computer. It simply means that the index has been changed. Forensic investigators are able to rebuild the index.

Key and Homberger argued that corporate IT experts do not have the legal background to understand the needs of forensic investigators. In other words, forensic investigation is a police issue, not an IT issue.

They used an example of a disgruntled employee using technology to steal a company's intellectual property. Forensic investigators may perform several tasks to catch such an employee: recovering damaged or deleted files; identifying and restoring files; identifying user-created files; searching the "slack" space areas of a hard drive, circumventing password protection and encryption; examining e-mails and temporary Internet files; identifying "cookies"; monitoring the computer network; and examining security log records. These actions, coupled with witness statements and timesheets, enable investigators to build a profile of the employee and follow the employee's actions.

Key and Homberger also described the potential of camera technology for catching dishonest employees. Older technology used photocells, videotape and "lots of wiring," they said. New technology is much simpler to employ and may specify what triggers a camera to activate - for example, someone tapping on a computer keyboard. This can then be monitored from practically anywhere. The technology can also be structured so that both the employee and the screen can be monitored at the same time.

However, they noted, the intrusive nature of these forensic investigations requires attention to the privacy expectations of employees - particularly when the investigation captures the activities of, or information about, third parties who have nothing to do with the conduct under investigation.

Investigating sexual harassment and romance in the workplace

Investigations into claims of workplace sexual harassment throw up some problematic dilemmas for employers when deciding the information which they can and cannot disclose.

"All workplaces are different. Every complaint is different. As a result, there is no set format for investigating sexual harassment complaints," cautioned Sue Paish, QC, a Vancouver-based lawyer whose practice centres on employment and human rights law.

Employers in Canada have a legal duty to deal with complaints of harassment that violate human rights codes. Despite the longstanding existence of sexual harassment policies in many Canadian workplaces, Paish stated, many employers may not be comfortable with the investigation or other processes involved in the policy.

Yet an effective investigation process promises several benefits, she said. It increases the likelihood of preventing other incidents, protects the company and employees from litigation and brings overall credibility to the harassment policy. Besides, it is the "right" thing to do.

Paish's presentation focussed on several aspects of investigating such complaints. At the heart of any good investigation, she noted, lies a good investigator acting solely as a fact-finder. A central need of the investigation process is the safeguarding of confidentiality. However, investigators may not be able to control what is done with personal information once it leaves their hands. Investigators should, therefore, get consent for what may be done with the information, to comply with any relevant legislation and legal obligations. Ideally, complainants should sign a form saying that they understand there may be a disclosure of information.

The complainant generally has no right to detailed information about measures taken to address the harassment. The complainant might be told only that measures have been taken to address the situation.

KEEPING CONFIDENTIALITY

No matter how well-designed a harassment process is, employees will not use it unless information is kept confidential, said Paish. Not only must the confidentiality of the complainant be protected, but also that of the respondent. Otherwise, the respondent is effectively being pre-judged. In addition, all participants in the investigation process should be assured that the information they provide will be kept confidential. However, there can be no anonymity in the complaints process, since the respondent has a right to know the identity of the complainant and a detailed description of the complaint.

By having a lawyer act as an external investigator, the report and information may be protected under the concept of legal privilege.

EXTERNAL INVESTIGATIONS

By having a lawyer act as an external investigator, Paish stated, the report and information may be protected under the concept of legal privilege. This may be particularly useful where data protection legislation might otherwise give parties rights of access to documents relating to the investigation.

Paish also advised employers to have a plan for handling evidence. The evidence should be kept after the investigation. It must be kept securely. It should be segregated from normal personnel files.

Employers may also need to be concerned about consensual office romances because of potential breaches of trust, conflicts of interest, or favouritism. However, unlike the United States, blanket anti-fraternisation rules are generally not upheld in Canada. Paish suggested that employers can instead rely on conflict of interest rules and disclosure policies to avoid potential problems, especially where there is a supervisor-supervised relationship.

Paish noted that under data protection legislation, such as the British Columbia Freedom of Information and Protection of Privacy Act, public sector employees who have been the subject of harassment complaints may apply to have the information collected during the investigation disclosed to them. However, she noted, a number of exceptions in the law often work to prevent harassment investigations from being disclosed. For example, information cannot be disclosed if doing so would harm the privacy of a third person.

Dealing with drug and alcohol incidents

Employers wanting to stamp out drug and alcohol abuse in the workplace will need to take into account a number of privacy safeguards if they wish to stay the right side of the law.

Victor Leginsky, a Vancouver-based management industrial relations lawyer, examined the motivation for employment drug testing and the privacy issues that flowed from testing. Drug testing, he argued, is becoming more common, but it must be considered against a backdrop of privacy and human rights laws and cases.

Employers, he said, have several motivations for an interest in workplace drug testing. They want maximum employee productivity and a safe working environment for employees and the public. Employers are entitled to manage their work sites and may prohibit alcohol and drugs and require employees to be unimpaired while at work. However, employees have a right to be free from employer intrusions into their off-duty lives.

Leginsky cautioned that it was important to "do the math". Are employees coming to work impaired or missing work due to alcohol or drugs? Employers must be able to defend a drug testing policy by demonstrating a problem caused by alcohol or drugs. Drug testing policies based simply on morality (he cited the US "war on drugs") will fail. Labour arbitrators look to see if the employer is being reasonable in all contexts. This also applies to decisions to introduce alcohol and drug testing.

He also warned of the obstacles confronting organisations that consider drug testing. Workers are already worried about the mass of data kept about them by employers. The results of drug testing will add to this, possibly revealing information not related to the purpose of the drug tests - the use of "recreational" drugs outside working hours, diabetes or pregnancy, for example. Being subjected to a drug test is possibly discriminatory, and also degrading, since employees must produce a urine sample while being watched to ensure validity of the sample. The tests themselves may also be unreliable.

Furthermore, alcohol and drug dependencies are considered disabilities under human rights laws in many jurisdictions. Employers have a duty to "accommodate" employees with disabilities, and dismissal based on alcohol or drug dependency may be prohibited under those laws.

Privacy legislation may add additional elements to the issue. Consent from those being tested may need to be more specific for the disclosure of health-related information (drug testing provides "health information") than for other types of personal information. Employers must build in specific consent for the collection of urine samples, and identify the disclosures of test results. Ideally, such consent should be obtained at the time of hiring a particular employee. Any drug testing policy must also explain its purpose, demonstrate the need for testing, the consequences of testing positive or refusing to be tested.

Leginsky cautioned that employers in Canada probably cannot require employees to be drug and alcohol-free 24 hours a day. He also reminded the audience that drug tests, unlike alcohol tests, cannot identify whether the employee was impaired at the time of the test. He suggested that it would be very difficult to justify pre-hiring or random testing as a "bona fide occupational requirement" under human rights legislation. However, random testing may be easier to justify in safety sensitive positions. "For cause" testing (for example, when an employee is seen drinking on the job) and post-accident/incident testing are more easily justified, as is testing on the return of an employee from an alcohol or drug treatment programme.