Internal Investigations, Data Analytics and Employee Privacy in Online/Computer Activity

Prepared for:

The Essential Privacy, Access to Information, CASL Forum

November 24, 2014

Dr. Andrea Slane

University of Ontario Institute of Technology

Internal Investigations into Employee Wrongdoing and Employee Online/Computer Privacy

- Wrongdoing discovered via system maintenance
  - Lessons from *R. v. Cole*
- Reasonableness of using "data analytics" to detect employee wrongdoing
  - Privacy concerns related to data analytics more generally
  - Debates regarding Bill C-13, *Protecting Canadians from Online Crime Act*
    - Passed by House of Commons October 20, 2014
    - Currently before the Senate
- Voluntary cooperation with police requests post-*Spencer*

Wrongdoing discovered via system maintenance

- *R. v. Cole,* 2012 SCC 53
  - Facts:
    - Defendant was a high school teacher and had administrator privileges over the computer network. He had discovered some nude images of a student while doing a system scan and saved them to his own hard drive, rather than telling the principal.
    - Another employee who likewise had admin privileges subsequently discovered the same images (for the same reason re compromised network integrity) on Cole's computer. He made a copy of the images and told the principle, who confiscated Cole's computer upon consulting with the school board. He called police, and turned the computer over to police for forensic analysis.

Wrongdoing discovered via system maintenance

- *R. v. Cole,* 2012 SCC 53
  - Main Issue:
    - Case concerned whether an employee had a reasonable expectation of privacy in his work-issued laptop, such that the police could not search the content of this computer based only on the employers consent (that is, without a warrant)
  - Secondary Issue:
    - If employees do have a reasonable expectation of privacy in their work-issued computer or other digital devices, does this impact the power of employers to monitor the employee's use of those devices and to examine their contents.

Wrongdoing discovered via system maintenance

- *R. v. Cole,* 2012 SCC 53
  - Decision:
    - Employees have a reasonable though diminished expectation of privacy in work issued computers if employers allow permit or can reasonably expect personal use of that device by the employee
      - Employee's expectation of privacy diminished by employer's policies that stated that the network was monitored and the contents were the property of the employer
      - Also diminished by "technological reality" (of which the employee was well aware) that the contents of the laptop could be remotely accessed whenever it was connected to the network
    - Result is that while employee's privacy interest is sufficient to protect him from warrantless police searches of the computer, the employer's interest in maintaining the network and investigating wrongdoing on the system/equipment was not affected and was reasonably exercised in this case

Management rights to employee computer use information: reasonableness standard

- PIPEDA requires that personal information may be collected, used and disclosed only for purposes that a reasonable person would find appropriate in the circumstances (s. 5(3) of PIPEDA)
- The Privacy Commissioner of Canada has set out a questions that should be considered in determining whether the collection, use or disclosure is reasonable:
  - Is the measure demonstrably necessary to meet a specific need?
  - Is it likely to be effective in meeting that need?
  - Is the loss of privacy proportional to the benefit gained?
  - Is there a less privacy-invasive way of achieving the same end?

Management rights to employee computer use information: reasonableness standard

- Much discussed complaint before the Alberta Privacy Commissioner in 2005: Parkland Regional Library:
  - Employer installed keystroke logging software to monitor the computer usage of an employee without his knowledge
  - Employer had concerns about low productivity and suspicions of his inappropriate use for personal purposes.
  - Commissioner found there was no legitimate reason for monitoring the employee this way:
    - insufficient evidence to support the employer's suspicions of wrongdoing
    - Keystroke logger not appropropriate to the productivity concerns
      - Provided much broader information about employee activities than necessary to meet that objective, so not the least intrusive way of collecting this information.
      - Alternative less intrusive methods for examining low productivity could have been employed, such as standard performance measures and review.

Management rights to employee computer use information: going forward

- 2005 is a long time ago in computer years
- Keystroke loggers are no longer the primary means of mining information about how people use computers – data analytics
- Important factors in that situation that may affect use of computer monitoring by employers:
  - Notice and Consent to be monitored as part of standard policy (absent in Parkland library), explaining purpose of monitoring
  - Commissioner did NOT find sufficient grounds to suspect wrongdoing (unauthorized personal use of computers) – could be different if there were sufficient grounds
    - Video surveillance has been justified where employer has reasonable grounds to suspect employee has breached employment terms or law – follows the same questions about reasonableness
    - Would condone computer use monitoring without consent on the same standard

“Big data” in the workplace: background

- Movement afoot to use data analytics in hiring, performance review, and disciplinary practices
- Some commentators describe the move to looking at more factors in hiring and promotion again as a pendulum swing back to a more “whole person” approach that includes personality, psychology and a range of other characteristics that have been formally off the table for a while
  - Don Peck article in The Atlantic last year asks:
    - “Should the ideas of scientists be dismissed because of the way they play a game? Should job candidates be ranked by what their Web habits say about them? Should the “data signature” of natural leaders play a role in promotion? These are all live questions today, and they prompt heavy concerns: that we will cede one of the most subtle and human of skills, the evaluation of the gifts and promise of other people, to machines; that the models will get it wrong; that some people will never get a shot in the new workforce.”

Big data in the workplace: privacy in public?

- Using Facebook in hiring: Dr. Donald Kluemper, Assistant Professor of Management at the University of Illinois at Chicago: http://vimeo.com/95038525
- Using online activity, in combination with personality and workplace specific (such as supervisor personalities, salaries, opportunities for promotion) to figure out who is likely to stay in a job and who is less likely
  - Concerns about discrimination entering in here
- Language and social interaction analytics: wearable badges that gather data on non-content information about conversations; or scan online communications to analyze patters that can be statistically correlated with success or failure in particular job roles

Big data in the workplace: uncovering wrongdoing via people analytics

- Using advanced data analytics to identify “fraud typologies” so as to periodically scan the organization’s systems to identify potential fraud to investigate

Reasonable expectations of privacy and data analytics

- Debates regarding “transmission data” in Bill C-13:
  - “transmission data” means data that
  - (*a*) relates to the telecommunication functions of dialling, routing, addressing or signalling;
  - (*b*) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is **generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication**; and
  - (*c*) does not reveal the substance, meaning or purpose of the communication.

Reasonable expectations of privacy and data analytics

- Debates regarding “transmission data” in Bill C-13:
  - Bill deems “transmission data” less sensitive than content data and has proposed new production orders on a lower standard than existing production orders:
    - Existing standard for production orders: reasonable grounds to believe that
      - (*a*) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;
      - (*b*) the documents or data will afford evidence respecting the commission of the offence; and
      - (*c*) the person who is subject to the order has possession or control of the documents or data
    - Proposed standard for transmission data production orders: reasonable grounds to suspect that
      - (*a*) an offence has been or will be committed under this or any other Act of Parliament;
      - (*b*) the identification of a device or person involved in the transmission of a communication will assist in the investigation of the offence; and
      - (*c*) transmission data that is in the possession or control of one or more persons whose identity is unknown when the application is made will enable that identification.

Reasonable expectations of privacy and data analytics

- Debates regarding “transmission data” in Bill C-13:
  - Significant amount of opposition to this approach to transmission data as less worthy of privacy protection: e.g. Privacy Commissioner of Canada
    - “Records of these sorts capture all manner of sensitive personal information that should be protected by an appropriately rigorous legal threshold. We believe suspicion will be too low a threshold for such revealing information in many cases, particularly in our digital era when every transaction, every message, every online search and every call or movement leaves a recorded trace and is, therefore, potentially subject to collection”
  - Bill C-13 is likely to be passed in its current form, but there are also likely to be legal challenges to this reduced standard on s. 8 grounds (right to be free from unreasonable search and seizure)
    - These challenges and their outcomes will inform our conceptions of what is a reasonable expectation of privacy re data analytics in other contexts as well – like the workplace

Responding to police requests for information about customers or employees

- *R. v. Spencer,* 2014 SCC 43 – released June 2014
  - Dealt with whether s. 487.014 of the Criminal Code, combined with s. 7(3)(c.1)(ii) of PIPEDA allowed police to ask an Internet service provider to supply the subscriber name and address of an account holder using a particular IP address at a particular date and time to commit child pornography offences
  - Held that the combination of these two provisions did not empower the police to legitimately ask for that sort of information, because it was sensitive enough (given that it unmasked a person's anonymous Internet activity) to require a warrant in most circumstances

Responding to police requests for information about customers or employees

- *R. v. Spencer,* 2014 SCC 43 – released June 2014
  - [73] Section 487.014(1) is a declaratory provision that confirms the existing common law powers of police officers to make enquiries, as indicated by the fact that the section begins with the phrase "[f]or greater certainty": see *Ward*, at para. 49. *PIPEDA* is a statute whose purpose, as set out in s. 3 , is to increase the protection of personal information. Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, I do not see how they could gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information.

Responding to police requests for information about customers or employees

- *R. v. Spencer,* 2014 SCC 43 – released June 2014
  - In the wake of this decision, most internet service providers have reportedly started requiring warrants, instead of providing subscriber information voluntarily upon police requests. The decision seems to say that if the information that is requested would normally require a warrant then police can't get it by way of s. 487.014 "in the absence of exigent circumstances or a reasonable law".
  - The government claims Bill C-13 is a "reasonable law" that would establish lower expectations of privacy in some forms of online data and would expressly affirm the right of police to ask for voluntary compliance with police requests….

Responding to police requests for information about customers or employees

- **Existing s. 487.014:**
- (1) For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.
- (2) A person who provides documents, data or information in the circumstances referred to in subsection (1) is deemed to be authorized to do so for the purposes of section 25.

- **Proposed s. 487.0195** (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.
- (2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so.

Thank-you

Please send any comments to

andrea.slane@uoit.ca