Privacy and Information Security Law

Elizabeth Ortmann-Vincenzo

CLASS 13

Employment Privacy;
International Privacy Law pt. 2

International Privacy Law pt. 2

2

D. THE APEC PRIVACY FRAMEWORK

The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. APEC's 21 members aim to create greater prosperity for the people of the region by promoting balanced, inclusive, sustainable, innovative and secure growth and by accelerating regional economic integration.

3

Cooperative Members

Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Viet Nam.

4

APEC Privacy Framework

- Like OECD guidelines
- Allows for exceptions to its principles
  - National sovereignty, national security, public safety, and public policy

5

APEC Privacy Framework Principles

1) preventing harm;
2) notice;
3) collection limitation;
4) use of personal information;
5) choice;
6) integrity;
7) security safeguards;
8) access and correction; and
9) accountability.

6

Implementation of APEC Privacy Framework: Cross Border Privacy Rules (CBPR)

- Voluntary accountability-based system
- Elements
  - (1) self-assessment; (2) compliance review; (3) recognition/ acceptance; and (4) dispute resolution and enforcement.
- Four participating APEC CBPR system economies: USA, Mexico, Japan and Canada

7

E. PRIVACY PROTECTION IN NORTH AMERICA

8

Canada

- Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000
  - "PIPEDA requires that the individual **must consent** prior to the collection, use, or disclosure of personal data. See id. sched. 1, §4.3. It also incorporates the OECD purpose specification principle, security safeguard principle, openness principle, accountability principle, and data quality principle, among others. PIPEDA has an unusual structure with its core found in its Schedule 1, which reprints most of the CSA Model Code."

9

Canada Anti-Spam Law (CASL)

- Effective in 2014
- CASL "prohibits sending unsolicited commercial emails. As a general matter, CASL requires express consent from a recipient before sending commercial emails. CASL does recognize, however, implied consent in situations where sender and recipient have an existing business relationship."

10

Mexico

- Mexican Constitution contains an explicit guarantee of privacy in private communications since 1996
- Federal Data Protection Act (FDPA) of 2010
  - Includes Habeas Data
- Privacy Notification Guidelines (2013)
  - Establish requirements for obtaining consent and providing privacy notices before data collection

11

F. PRIVACY PROTECTION IN SOUTH AMERICA

12

Argentina

- Law of the Protection of Personal Data (2000)
- **Habeas data** – "permits any person to know the content and purpose of the data pertaining to her in public records, or in certain private records"
- Prohibits international transfer of PI to countries without adequate protection

13

Brazil

- Constitution explicitly protects privacy
- Habeas data

14

G. PRIVACY PROTECTION IN AFRICA AND THE MIDDLE EAST

15

Africa

- A number of countries now have data protection laws
- South Africa
  - 1996 Constitution grants a right to privacy
  - 2013 Protection of Personal Information Act

16

The Middle East

- Some Arab countries mention privacy
- 2002 Dubai law restricts ISPs from disclosing customer data
- Israel
  - Article 7 provides for a right to privacy
  - Privacy Protection Act of 1981
    - Applies to public and private sector
    - Prohibits use of information in a database for purposes beyond for which it was established

17

H. PRIVACY PROTECTION IN ASIA-PACIFIC

18

Australia

- Privacy Protection Act of 1988 based on OECD Privacy Guidelines
  - Applies only to the public sector
- Privacy Amendment Act of 2000
  - Applies to the private sector
- Additional amendments became effective March 2014
  - Regulates handling of personal information and credit reporting

19

Japan

- Personal Data Protection Act effective 2005
  - Personal information may be collected with a purpose of use that cannot be exceeded
  - Right to request disclosure of stored personal information on the user

20

China

- Protections for privacy include defamation, home intrusion, and correspondence monitoring
- Extensive citizen monitoring
- Yinsi (shameful secret)
- 2011 draft guidelines for information security technology

21

Hong Kong

- Information privacy statute enacted in 1996
  - Regulates public and private sector
  - Privacy commissioner
- Revisions to Personal Data Ordinance in 2013
  - Consent required prior to use of personal data in targeted marketing

22

South Korea

- Personal Information Protection Act effective 2012
  - Applies to public and private sector
  - Requires Privacy Compliance officers, notification of data breach, only minimum collect of personal information occur

23

India

- Constitutional right to privacy
- 2008 IT Security Act
  - First Indian data privacy law
    - Requires establishment of a privacy policy and more

24

Employment Privacy

25

Employee Surveillance and Testing

- Reasons
  - Hire workers who are not likely to cause disruptions or be careless and reckless
  - Increase productivity
  - Curtail employee misconduct
  - Investigate particular incidents of misconduct

26

Public Sector Employees

- 4th Amendment
- State constitutions
- Federal and state wiretap law
- Americans with Disabilities Act (ADA)
- Federal Privacy Act
- Privacy invasions under privacy torts

27

Private Sector Employees

- Similar to public sector employees
  - 4th Amendment and most state constitutions do not apply
- Potentially additional contractual remedies

28

A. WORKPLACE SEARCHES

29

O'Connor v. Ortega

- 1987 Supreme Court
- Issue
  - 4th Amendment rights of public employees
- Diminished expectation of privacy in the workplace

30

O'Connor v. Ortega

- "The strictures of the Fourth Amendment, applied to the States through the Fourteenth Amendment, have been applied to the conduct of governmental officials in various civil activities. …Thus, we have held in the past that the Fourth Amendment governs the conduct of school officials, building inspectors, and Occupational Safety and Health Act inspectors. . . . **Searches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment**."

31

O'Connor v. Ortega

- "Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. **The workplace includes those areas and items that are related to work and are generally within the employer's control.** At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board."

32

O'Connor v. Ortega

- "The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address."

33

O'Connor v. Ortega

- "The employee's expectation of privacy must be assessed in the context of the employment relation. … [T]he question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. …"

34

O'Connor v. Ortega

- "We hold, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the **standard of reasonableness** under all the circumstances."

35

Kmart v. Trotti: Employee Lockers

- "[B]y having placed a lock on the locker at the employee's own expense and with the appellants' consent, has demonstrated a **legitimate expectation to a right of privacy in both the locker itself and those personal effects** within it."

36

B. WORKPLACE SURVEILLANCE

37

Thompson v. Johnson County Community College

- 1996 District Court of Kansas
- Issue
  - Does video surveillance of a locker area violate federal wiretap law and the 4th Amendment?

38

Thompson v. Johnson County Community College

- "**Domestic silent video surveillance is subject to Fourth Amendment prohibitions against unreasonable searches**. However, this does not mean that defendants' use of video surveillance automatically violated plaintiffs' Fourth Amendment rights. Rather, the court first must determine whether plaintiffs had a **reasonable expectation of privacy** in their locker area. If plaintiffs had no reasonable expectation of privacy in this area, there is 'no fourth amendment violation regardless of the nature of the search.'"

39

Thompson v. Johnson County Community College

- No reasonable expectation of privacy in a security personnel locker area
  - Not enclosed
  - Viewable by anyone
  - Not reserved exclusively for use of the personnel

40

Surveillance Outside the Workplace

- "Defendants' surveillance of plaintiff at his home involved matters which defendants had a legitimate right to investigate. … **Plaintiff's privacy was subject to the legitimate interest of his employer in investigating suspicions that plaintiff's work-related disability was a pretext**. We conclude that plaintiff does not meet the second requirement of the intrusion into seclusion test. Defendant also has a right to investigate matters that are potential sources of legal liability."
- Saldana v. Kelsey-Hayes

41

C. WORKPLACE DRUG TESTING

42

National Treasury Employees Union v. Von Raab

- 1989 Supreme Court
- Issue
  - Required drug tests for certain employees of Custom Services
- Drug tests are a condition of employment for:

1) Drug interdiction employees
2) Employees carrying firearms
3) Employees handling classified materials

43

National Treasury Employees Union v. Von Raab

- "Customs employees who test positive for drugs and who can offer no satisfactory explanation are subject to dismissal from the Service. Test results may not, however, be turned over to any other agency, including criminal prosecutors, without the employee's written consent."

44

National Treasury Employees Union v. Von Raab

- "Our precedents have settled that, in certain limited circumstances, the Government's need to discover such **latent or hidden conditions**, or to prevent their development, is **sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion**. We think the Government's need to conduct the suspicionless searches required by the Customs program outweighs the privacy interests of employees engaged directly in drug interdiction, and of those who otherwise are required to carry firearms."

45

D. THE ISSUE OF CONSENT

46

Employee Notice

- "[T]he Court finds that the taking of urine samples is an intrusion in an area in which plaintiffs may have an expectation of privacy. However, in this case, the Court finds that **plaintiffs had no expectation of privacy with regard to drug testing since they had been on notice**…"
- Baggs v. Eagle-Picher Industries

47

Requiring Employee Consent

- "[C]ourts have [generally] held that employers requiring employees to consent to drug testing (or to surveillance or monitoring) shield themselves from liability under the intrusion upon seclusion tort because the employees consented to the intrusion."

48

E. TESTING, QUESTIONNAIRES, AND POLYGRAPHS

49

Interrogations under the 4th Amendment

- "The Fourth Amendment was not drafted, and has not been interpreted, with interrogations in mind. …. Our conclusion that the plaintiff has not stated a Fourth Amendment claim does not leave people … remediless. States are free to protect privacy more comprehensively than the Fourth Amendment commands; and [the plaintiff] is free to continue to press her **state-law claims in state court**, where they belong. In most states if [] officials were to publicize highly personal information obtained … by the kind of test of which she complains, she would have a state-law claim for invasion of her tort right of privacy."
- Greenawalt v. Indiana Department of Corrections, 7th Cir. 2005

50

NASA v. Nelson

- 2011 Supreme Court
- Issue
  - Rights violation for form questionnaire with drug-related questions and open ended questions to references

51

NASA v. Nelson

- "We hold [] that, whatever the scope of this interest, it does not prevent the Government from asking reasonable questions [on forms included] in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure."

52

NASA v. Nelson

- "The Privacy Act, which covers all information collected during the background-check process, allows the Government to maintain records 'about an individual' only to the extent the records are **'relevant and necessary to accomplish' a purpose** authorized by law. 5 U.S.C. §552a(e)(1). The Act requires **written consent before the Government may disclose** records pertaining to any individual. §552a(b). And the Act imposes **criminal liability** for willful violations of its nondisclosure obligations. §552a(i)(1). … Like the protections against disclosure in *Whalen* and *Nixon,* they 'evidence a proper concern' for individual privacy."

53

Polygraph Testing

- Recordation of three physiological responses:
  - Galvanic skin response
  - Relative blood pressure
  - Respiration

54

The Employee Polygraph Protection Act

- Passed in 1988
- Applies only to private employees and not government employees
- Employers cannot use polygraphs unless (i) ongoing investigation, (ii) employee had access to property under investigation, (iii) reasonable suspicion that the employee is involved, and (iv) employer executed statement

55

F. TELEPHONE MONITORING

56

Employer Exceptions

1) Consent to the interception
2) Permitted to intercept, disclose, or use that communication as a necessary incident to render the service or to protect the rights or property of the service
3) Ordinary course of business exception

57

Watkins v. L.M. Berry & Co.

- 1983 11th Cir.
- Issue
  - Monitoring of employee's calls revealed an interview with another company

58

Watkins v. L.M. Berry & Co.

- "It is not disputed that Little's conduct violates section 2511(1)(b) unless it comes within an exemption 'specifically provided in' title III (18 U.S.C. §2511(1)). Appellees claim the applicability of two such exemptions."

1. Consent exemption
2. Business extension exemption

59

Watkins v. L.M. Berry & Co.

- "The consent and business extension exemptions are analytically separate. **Consent may be obtained for any interceptions**, and the business or personal nature of the call is entirely irrelevant. Conversely, **the business extension exemption operates without regard to consent**. So long as the **requisite business connection** is demonstrated, the business extension exemption represents the 'circumstances under which non-consensual interception' is not violative of section 2511(1)(b)."

60

Watkins v. L.M. Berry & Co.

- "We hold that **a personal call may not be intercepted in the ordinary course of business** under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not."

61

Deal v. Spears

- 1992 8th Cir.
- Issue
  - Recordation of phone calls on a mixed business and personal line of the employer

62

Deal v. Spears

- "The elements of a violation of the wire and electronic communications interception provisions (Title III) of the Omnibus Crime Control and Safe Streets Act of 1968 are set forth in the section that makes such interceptions a criminal offense. 18 U.S.C. §2511 (1988). Under the relevant provisions of the statute, criminal liability attaches and a federal civil cause of action arises **when a person intentionally intercepts a wire or electronic communication or intentionally discloses the contents of the interception**."
- Possible consent exception or business use of a telephone exemption

63

G. COMPUTER MONITORING AND SEARCHES

64

Work Email Privacy Expectations

- How should an employee's reasonable expectation of privacy be assessed for work email?

65

Work Email

- "[W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."
- Smith v. Pillsbury Co. (E.D.PA 1996)

66

Work-Related Email Liability

- Defamation
- Copyright infringement
- Sexual harassment

67

Service Provider Exception

- "In many workplaces — such as government workplaces, universities, and large corporations — the employers are also the **service providers**. Therefore, they would be **exempt from intercepting e-mail under the Wiretap Act**. Additionally, employers can have employees **sign consent forms** to the monitoring, and consent is an exception to federal wiretap law."

68

Social Media Password Demands

- Reasonable expectation of privacy in privately posted messages in social media
- Several states have passed laws to prohibit schools and/or employers from demanding social media passwords

69

U.S. v. Ziegler

- 9th Cir. 2007
- Issue
  - Does an employer's coordination with the FBI regarding a child pornography investigation including copying a work hard drive violate an employee's privacy rights?

70

U.S. v. Ziegler

- Defendant's groups for appeal:
- "[T]he January 30, 2001, entry into [D's] private office to search his workplace computer violated the Fourth Amendment and, as such, the evidence contained on the computer's hard drive must be suppressed."

71

U.S. v. Ziegler

- "[A] criminal defendant may invoke the protections of the Fourth Amendment only if he can show that he had a *legitimate* expectation of privacy in the place searched or the item seized."

72

U.S. v. Ziegler

- Did D have a legitimate expectation of privacy?
  - "Ziegler's expectation of privacy in his office was reasonable on the facts of this case. His office was not shared by co-workers, and kept locked.
  - "Because Ziegler had a reasonable expectation of privacy in his office, any search of that space and the items located therein must comply with the Fourth Amendment."

73

U.S. v. Ziegler

- "[Was] the search of Ziegler's office and the copying of his hard drive were "unreasonable" within the meaning of the Fourth Amendment [?] As in *Mancusi,* the government does not deny that the search and seizure were without a warrant, and 'it is settled for purposes of the Amendment that "except in certain carefully defined classes of cases, **a search of private property without proper consent is 'unreasonable' unless it has been authorized by a valid search warrant**.'"

74

U.S. v. Ziegler

- Consent is an exception to the government's warrant requirement
- Consent may be given by the party to be searched, or a "third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected"

75

U.S. v. Ziegler

- What about computer consent?
- "[An employer" could give valid consent to a search of the contents of the hard drive of [an employee's] workplace computer because the computer is the type of workplace property that remains within the control of the employer 'even if the employee has placed personal items in [it].'"

76

U.S. v. Ziegler

- "The remaining question is, given [the employer's *ability* to consent to a search, did it consent to a search of the office and the computer. We conclude that it did. … And because valid third party consent to search the office and computer located therein was given by his employer, the district court's order denying suppression of the evidence of child pornography existing on [Defendant's] computer is affirmed."

77

Duty to Monitor Employees

- Are there policies in place to monitor the employee's use of email and the Internet?
  - "We hold that an **employer who is on notice** that one of its employees is using a workplace computer to access pornography, possibly child pornography, **has a duty to investigate the employee's activities** and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third parties. No privacy interest of the employee stands in the way of this duty on the part of the employer. …"
- Doe v. XYC Corp.

78

Program Completed

79