Privacy and Information Security Law

Randy Canis

CLASS 12

Financial Data pt. 2;
Employment Privacy
Financial Data pt. 2

B. THE GRAMM-LEACH-BLILEY ACT

Gramm-Leach-Bliley

- Allows for sharing of personal information by financial institutions
- Only protects financial information that is not public
- Affiliates of the organization can share personal information by telling customers with a general disclosure policy
Sharing with Nonaffiliated Companies

• Financial institutions can share personal information with nonaffiliated companies for broad purposes if individuals are provided an opportunity to first opt out.

Security Program

• “According to the regulations, financial institutions ‘shall develop, implement, and maintain a comprehensive information security program’ that is appropriate to the ‘size and complexity’ of the institution, the ‘nature and scope’ of the institution’s activities, and the ‘sensitivity of any customer information at issue.’ 16 C.F.R. §314.3(a). An ‘information security program’ is defined as ‘the administrative, technical, or physical safeguards [an institution uses] to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information.’ §314.2(b).”

Preemption

• “GLBA does not preempt states laws that provide greater protection to privacy.”
GLBA Summary

1. Financial institutions are required to establish and implement procedures keeping nonpublic personal information confidential and protecting the information from unauthorized use;
2. Customers must receive an annual notice detailing how nonpublic personal information is protected and on what basis information is shared;
3. Customers must be given the right, though not absolute, to opt-out of information sharing;
4. Fraudulently obtaining or using nonpublic personal information is a federal crime;
5. While the courts are split, states may not regulate the sharing of information included in the definition of consumer report contained in the FCRA;
6. A financial institution, despite GLBA restrictions, is expected to respond to information requests made as part of the judicial process.

Privacy Law in a Nutshell, 2nd Edition

C. FEDERAL AND STATE FINANCIAL PRIVACY LAWS
Bank Secrecy Act

• "Regulations promulgated under the Act by the Secretary of the Treasury require reporting to the government of financial transactions exceeding $10,000 if made within the United States and exceeding $5,000 if into or out of the United States."

Identity Theft Assumption and Deterrence Act

• "The Act makes it a federal crime to ‘knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.’ 18 U.S.C. §1028."

Actions Against Credit Card Companies

• "With the alarming increase in identity theft in recent years, commercial banks and credit card issuers have become the first, and often last, line of defense in preventing the devastating damage that identity theft inflicts. Because the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, the Court finds that under Tennessee negligence law, Defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card. The Court, however, emphasizes that this duty to verify does not impose upon Defendant a duty to prevent all identity theft."

• Wolfe v. MBNA America Bank
Employment Privacy

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

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
Private Sector Employees

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

A. WORKPLACE SEARCHES

O’Connor v. Ortega

- 1987 Supreme Court
- Issue
  - 4\textsuperscript{th} Amendment rights of public employees
O’Connor v. Ortega

• Accusations against Ortega’s residency program
  – Misleading officials
  – Coerced contributions
  – Sexual harassment
  – Inappropriate disciplinary actions

• Thorough search made of Ortega’s office

• “Dr. Ortega commenced this action against petitioners in Federal District Court under 42 U.S.C. §1983, alleging that the search of his office violated the Fourth Amendment.”

• “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.”
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."

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."

O'Connor v. Ortega

"The employee's expectation of privacy must be assessed in the context of the employment relation. ... The question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. ..."
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.”

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.”

B. WORKPLACE SURVEILLANCE
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?

---

"Under Title I, ‘any person whose wire or oral communications is intercepted, disclosed or used in violation of [the Act] may in a civil action recover from the person or entity which engage in that violation such relief as may be appropriate.’ 18 U.S.C. §2520"

---

Thompson v. Johnson County Community College

- Silent video – Title I doesn’t prohibit its use
- Video including audio – violates Title I
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.""

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

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
C. WORKPLACE DRUG TESTING

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
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.”

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.”

Borse v. Piece Goods Shop

• 1992 3rd Circuit
• Issue
  – “[W]hether an at-will employee who is discharged for refusing to consent to urinalysis screening for drug use and to searches of her personal property states a claim for wrongful discharge under Pennsylvania law…”
Borse v. Piece Goods Shop

• Employee refused to sign the consent form
• Company terminated employee’s employment

Borse v. Piece Goods Shop

• PA Intrusion on Seclusion
  – “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts §652B.…”

Borse v. Piece Goods Shop

• Urinalysis possible violations
  1) Manner in which the program is conducted (e.g., collection of urine)
  2) Disclosing private medical facts
D. THE ISSUE OF CONSENT

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

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.”
E. TESTING, QUESTIONNAIRES, AND POLYGRAPHS

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

NASA v. Nelson

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

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.”

Polygraph Testing

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

F. TELEPHONE MONITORING

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
Watkins v. L.M. Berry & Co.

• 1983 11th Cir.
• Issue
  – Monitoring of employee’s calls revealed an interview with another company

“...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

“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).”
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.”

Deal v. Spears

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

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
Work Email Privacy Expectations

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

---

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)
Work-Related Email Liability

- Defamation
- Copyright infringement
- Sexual harassment

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.”

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
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?

U.S. v. Ziegler

- Employer tipped FBI that D had accessed child porn websites from work
- Employer monitored workplace computers and employees were aware of the monitoring
- Employer made a copy of the employee’s hard drive (at direction of the FBI?)

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.”
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.”

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.”

U.S. v. Ziegler

• “[W]as 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.”
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”

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].”

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.”
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.