Privacy and Information Security Law

Randy Canis

CLASS 14 pt. 2

Final Review

Final Exam Info

- Final Exam format
  - 50 multiple choice questions + bonus questions
  - 2 points per question
  - All answers to be completed in Excel document provided on website
  - Use capital letters for your answer

2

Final Exam Info

- Grading
  - I will not acknowledge receipt of your graded exam immediately.
  - However, I will respond within 24 hours of receipt of your exam with your final grade
  - I will not advise you of which questions you scored correctly or incorrectly on the final exam, nor do I send an answer key
  - However, if you did not receive the grade you expected to receive, I am willing to go over the questions with you that you missed.

3

Final Exam Info

- Thus, you have an incentive to turn in the final exam early so that you can get your grade early and address any issues before your final exam grade is entered.
- I reserve my right to enter final grades for all students at 12:01 p.m. the day the exam is due.
- DO NOT BE LATE IN TURNING IN THE EXAM OR, AMOUNG OTHER THINGS, YOUR GRADE IN THE COURSE COULD BE DELAYED
- Any further questions about the final exam?

4

Final Review

- What did we learn this semester?
- Let's review…

5

Branches of U.S. Government (3)

	Legislative	Executive	Judicial
Body	**Congress**	**Pres & Admin Agencies**	**Federal Courts**
Role	**"Make"**	**"Enforce"**	**"Interpret"**
"Product"	**Statutes**	**Regulations**	**Case Opinions**
Location	**U.S. Code**	**Federal Register and C.F.R.**	**Case Reporters**

6

Federal Court Structure

- US Supreme Court (1)
- US Court of Appeals (13)
  - 8th Circuit
  - Federal Circuit
- US District Courts (144); at least 1 per state
  - Missouri - 2 Federal District Courts
    - Eastern District - St. Louis
    - Western District - Kansas City
    - + Federal Bankruptcy Court

7

Any Questions?

- See you for the final class next week…

8

Warren and Brandeis Article

- General right of the individual to be let alone
- "[T]he existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."

9

Prosser Article

- "Taking them in order — intrusion, disclosure, false light, and appropriation — the first and second require the invasion of something secret, secluded or private pertaining to the plaintiff; the third and fourth do not. The second and third depend upon publicity, while the first does not, nor does the fourth, although it usually involves it. The third requires falsity or fiction; the other three do not. The fourth involves a use for the defendant's advantage, which is not true of the rest."

10

Lake v. Wal-Mart Stores, Inc.

- "Today we join the majority of jurisdictions and **recognize the tort of invasion of privacy**. The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close…"

11

Privacy Protection in Tort Law

1) Public Disclosure of Private Facts.
2) Intrusion upon Seclusion.
3) False Light.
4) Appropriation.

12

Public Disclosure of Private Facts

- "This tort creates a cause of action for one who publicly discloses a private matter that is 'highly offensive to a reasonable person' and 'is not of legitimate concern to the public.'"
- Restatement (Second) of Torts §652D (1977).

13

Intrusion upon Seclusion

- "This tort provides a remedy when one intrudes 'upon the solitude or seclusion of another or his private affairs or concerns' if the intrusion is 'highly offensive to a reasonable person.'"
- Restatement (Second) of Torts §652B (1977).

14

False Light

- "This tort creates a cause of action when one publicly discloses a matter that places a person 'in a false light' that is 'highly offensive to a reasonable person.'"
- Restatement (Second) of Torts §652E (1977).

15

Appropriation

- "Under this tort, a plaintiff has a remedy against one 'who appropriates to his own use or benefit the name or likeness' of the plaintiff."
- Restatement (Second) of Torts §652C (1977).

16

Four Types of Media Privacy Incursions

- (1) intrusions and harassment in the course of gathering information;
- (2) the disclosure of truthful information,
- (3) the dissemination of misleading or false information; and
- (4) the appropriation of name or likeness.

17

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 §652B

18

Shulman v. Group W Productions, Inc.

- "[T]he action for intrusion has two elements:
  (1)intrusion into a private place, conversation or matter,
  (2)in a manner highly offensive to a reasonable person."

19

Video Voyeurism Prevention Act

- (a) Whoever, in the special maritime and territorial jurisdiction of the United States, having the **intent to capture** an improper image of an individual, **knowingly does so** and that individual's naked or undergarment clad genitals, pubic area, buttocks, or female breast is depicted in the improper image under circumstances in which that individual has a **reasonable expectation of privacy** regarding such body part or parts, shall be fined under this title or imprisoned not more than one year, or both.

20

Publicity Given to Private Life

- One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

  (a) would be **highly offensive** to a reasonable person, and

  (b) is **not of legitimate concern** to the public

21

Newsworthiness Tests

1) Leave it to the press
2) Customs and conventions of the community
3) Nexus test

22

Shulman v. Group W Productions

- "[U]nder California common law the dissemination of truthful, **newsworthy material is not actionable as a publication of private facts**. If the contents of a broadcast or publication are of legitimate public concern, the plaintiff cannot establish a necessary element of the tort action, the lack of newsworthiness. …"

23

Shulman v. Group W Productions

- "[C]ourts have generally protected the privacy of otherwise private individuals involved in events of public interest 'by requiring that a **logical nexus** exist between the complaining individual and the matter of legitimate public interest.'"

24

The Florida Star v. B.J.F.

- "We hold [] that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order …"

25

Defamation

- Defamation occurs when one's words reflect negatively upon another person's integrity, character, good name and standing in the community and those words tend to expose the other person to public hatred, contempt or disgrace. … Defamation includes both libel and slander.
- **Libel** – writing or other permanent form
- **Slander** – orally
- See Missouri Bar's News Reports Handbook.

26

Libel v. Slander

- (1) **Libel** consists of the publication of defamatory matter by **written or printed words**, by its embodiment in physical form or by any other form of communication that has the potentially harmful qualities characteristic of written or printed words.
- (2) **Slander** consists of the publication of defamatory matter by **spoken words**, transitory gestures or by any form of communication other than those stated in Subsection (1).
- Restatement §568.

27

Publisher and Distributor Liability

- **Publisher liability** – repeating or publishing the libelous statements of others
- **Distributor liability** – merely disseminating a libelous statement
  - Distributors cannot be found liable unless they knew or had reason to know about the defamatory statement

28

Communications Decency Act

- Immunizes online service providers from postings, e-mails, and other Internet contributions made by others
- Section 230 of CDA "No provider … of interactive computer services shall be treated as the publisher or speaker of any information provided by another information content provider"

29

Zeran v. America Online, Inc.

- Does this mean Internet service providers should not remove offensive or infringing content?
  - "Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. … [] § 230 **forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions**."

30

Public Figures

- Public figures are "fair game" and false and defamatory statements about them that are published in the press will not constitute defamation unless the statements are made with actual malice
- **Actual malice** – with either knowledge of its falsity or a reckless disregard of the truth

31

Defense

- Truth is normally an absolute defense
- Privilege
  - **Absolute** – judicial proceedings and certain government proceedings
  - **Conditional** – certain statements made in good faith and the publication is limited to those who have a legitimate interest in the communication

32

False Light v. Defamation

- **Defamation** – reputational injury; communication to another person
- **False Light** – exclusively for emotional distress; wider communication

33

Infliction of Emotional Distress

- One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm.

34

Appropriation of Name or Likeness

- One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.

35

Jordan v. Jewel Food Stores, Inc.

- "But an ad congratulating a famous athlete **can only be understood as a promotional device for the advertiser**. Unlike a community group, the athlete needs no gratuitous promotion and his identity has commercial value. Jewel's ad cannot be construed as a benevolent act of good corporate citizenship."

36

"Real Relationship" Test

- "A picture illustrating an article on a matter of public interest is not considered used for the purpose of trade or advertising within the prohibition of the statute **unless it has no real relationship to the article, or unless the article is an advertisement in disguise**. … The test of permissible use is not the currency of the publication in which the picture appears but whether it is illustrative of a matter of public interest."

37

Anonymity

- "Anonymity (or the use of pseudonyms) involves people's ability to conduct activities without being identified."
  - Invocation of 1st Amendment right to protect oneself from being identified.
  - When should anonymity be removed?

38

Constitutional Regulatory Regime

- The Fourth and Fifth Amendments significantly limit the government's power to gather information.
  - **4th** – "regulates the government's activities in searching for information or items as well as the government's seizure of things or people."
  - **5th** – "guarantees that '[n]o person . . . shall be compelled in any criminal case to be a witness against himself. …' The Fifth Amendment establishes a 'privilege against self-incrimination,' and it prohibits the government from compelling individuals to disclose inculpatory information about themselves."

39

4th Amendment Issues

1) Is the government's information collecting regulated by the 4th Amendment?
2) Is the search or seizure reasonable?
3) What is the result of the 4th Amendment violation?

40

Reasonable Searches and Seizures

- The 4th amendment does not bar searches and seizures, but requires that they be "reasonable".
  - "Generally, a search or seizure is reasonable if the police have obtained a **valid search warrant**. To obtain a warrant, the police must go before a judge or magistrate and demonstrate that they have '**probable cause**' to conduct a search or seizure."

41

Katz v. United States

- "'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that **searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment** — subject only to a few specifically established and well-delineated exceptions…"

42

Katz v. United States

- "[F]irst that a **person have exhibited an actual (subjective) expectation of privacy** and, second, that the **expectation be one that society is prepared to recognize as 'reasonable.'** Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."

43

"Reasonable Expectation" or Privacy Test

1) A person must exhibit an actual (subjective) expectation of privacy and
2) The expectation must be one that society is prepared to recognize as "reasonable".

44

Electronic Communications Privacy Act (ECPA)

1) Wiretap Act
   - Communications in transmission
2) Stored Communication Act (SCA)
   - Communications in storage
3) Pen Register Act

Passed in 1986; amended Title III

45

Computer Searches at the Border

- Government does not need a warrant or even reasonable suspicion to justify searches of a person or property at an international border

46

Riley v. California

- Reasonableness of a warrantless search incident to an arrest
  - "When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to **remove any weapons** that the latter might seek to use in order to resist arrest or effect his escape . . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any **evidence on the arrestee's person** in order to **prevent its concealment or destruction.** …"

47

United States v. Warshak

- "[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored with, or sent or received through, a commercial ISP." **The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause**. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional. …"

48

United States v. Forrester

- "[E]-mail and Internet users have **no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit** because they should know that this information is provided to and **used by Internet service providers** for the specific purpose of directing the routing of information. … [E]-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are **voluntarily turned over** in order to direct the third party's servers."

49

New Jersey v. T.L.O.

- "[S]chool officials **need not obtain a warrant** before searching a student who is under their authority. … . [T]he legality of a search of a student should depend simply on the reasonableness, under all the circumstances, of the search. Determining the reasonableness of any search involves a twofold inquiry: first, one must consider '**whether the . . . action was justified at its inception**'; second, one must determine **whether the search** as actually conducted '**was reasonably related in scope** to the circumstances which justified the interference in the first place.'"

50

Board of Education v. Earls

- "In Vernonia, this Court held that the suspicionless drug testing of athletes was constitutional. The Court, however, did not simply authorize all school **drug testing**, but rather conducted a **fact-specific balancing of the intrusion on the children's Fourth Amendment rights against the promotion of legitimate governmental interests**. Applying the principles of Vernonia to the somewhat different facts of this case, we conclude that Tecumseh's Policy is also constitutional…"

51

The Family Education Rights and Privacy Act

- "The Family Educational Rights and Privacy Act … generally prohibits schools from releasing student **'education records'** without the authorization of the student and/or parent. Schools may release such **'directory' information** as names, addresses, dates of attendance, degrees earned, and activities unless the student and/or parent expressly indicates in writing that he or she wants it to remain confidential."

52

Privacy Policies

- Part of self-regulation
- "[Privacy] policies describe the information that is collected, how it will be used and shared, and how it will be safeguarded. Consumers are sometimes offered a choice to opt-out of some uses of their data."

53

FTC's View

- "Since the late 1990s, the Federal Trade Commission (FTC) has deemed **violations of privacy policies to be an 'unfair or deceptive' practice under the FTC Act**. The FTC has the power to enforce the FTC Act. The result of the FTC's involvement has been to create a system of quasi-self-regulation, where **companies define the substantive terms** of how they will collect, use, and disclose personal data, but they are then **held accountable to these terms by the FTC**. Over time, however, the FTC has interpreted the FTC Act as requiring more of companies than merely following promises."

54

Pineda v. Williams-Sonoma Stores

- Section 1747.08, subdivision (a) provides, in pertinent part, "[N]o person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall . . . : (2) **Request, or require as a condition to accepting the credit card** as payment in full or in part for goods or services, the cardholder to provide **personal identification information**, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise. Subdivision (b) defines personal identification information as "information concerning the cardholder, **other than information set forth on the credit card**, and including, but not limited to, the cardholder's address and telephone number."

55

Dwyer v. American Express Co.

- Issue
  - Is Amex liable for invasion of privacy and consumer fraud for its practice of renting information regarding cardholder spending habits?
- Answer
  - No

56

FTC Consent Decrees

- Elements include "(1) **prohibition on the activities** in violation of the FTC Act; (2) **steps to remediate** the problematic activities, such as software patches or notice to consumers; (3) **deletion** of wrongfully-obtained consumer data; (4) **modifications to privacy policies**; (5) **establishment of a comprehensive privacy program**, including risk assessment, appointment of a person to coordinate the program, and employee training, among other things; (6) **biennial assessment reports** by independent auditors; (7) **recordkeeping** to facilitate FTC enforcement of the order; (8) **obligation to alert** the FTC of any material changes in the company that might affect compliance obligations (such as mergers or bankruptcy filings)."

57

Types of Section 5 Privacy and Security Violations

- "Deception" prong
  - "FTC brings cases for broken promises of privacy, general deception, insufficient notice, and unreasonable data security practices."

58

Types of Section 5 Privacy and Security Violations

- "Unfairness" prong
  - "[T]he FTC brings cases for retroactive changes to privacy policies, deceitful data collection, improper use of data, unfair design or unfair default settings, and unfair data security practices."

59

Nguyen v. Barnes & Noble Inc.

- "Because no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website, the determination of the validity of the browsewrap contract depends on whether the user has actual or constructive knowledge of a website's terms and conditions."

60

Sources for the Right of Action

1) state physician licensing statutes,
2) evidentiary rules and privileged communication statutes which prohibit a physician from testifying in judicial proceedings,
3) common law principles of trust, and
4) the Hippocratic Oath and principles of medical ethics which proscribe the revelation of patient confidences.

McCormick v. England, (S.C.Ct. App. 1997)

61

Exceptions to the Tort

- "One important exception to the tort is that physicians will not be liable for disclosing confidential medical information **when it is necessary to protect others from danger or when it is required by law**."

62

Protection of Intended or Potential Victim

- "[T]his court holds that a psychiatrist or therapist may have a **duty to take whatever steps are reasonably necessary to protect** an intended or potential victim of his patient when he determines, or should determine, in the appropriate factual setting and in accordance with the standards of his profession established at trial, that the patient is or may present a probability of danger to that person. The relationship giving rise to that duty may be found either in that **existing between the therapist and the patient**, as was alluded to in *Tarasoff*, or in the more broadly based **obligation a practitioner may have to protect the welfare of the community**, which is analogous to the obligation a physician has to warn third persons of infectious or contagious disease."

63

HIPAA

- What is HIPAA?
  - Health Insurance Portability and Accountability Act of 1996
  - Privacy Rule
    - addresses the use and disclosure of individuals' health information
  - Security Rule
    - Requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address them

64

Protected Health Information

- **Protected Health Information** (PHI) is all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media

65

Business Associates

- A **business associate** is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.
- From HHS Summary of the HIPAA Privacy Rule

66

Business Associate Agreement

- A covered entity needs a business associate agreement with another company that is providing "business associate" services on its behalf
- Business associate agreement must be in writing and provide for safeguarding of individually identifiable health information provided by the covered entity to the business associate

67

Who is Covered by the Privacy Rule?

- Covered
  - Health plans
  - Health care clearinghouses
    - Billing services, re-pricing companies, etc.
  - Health care providers that transmit health information in electronic form
- If covered, you are deemed a **covered entity**.

68

General Use and Disclosure

- A covered entity may only use PHI as permitted under the Privacy Rule or as authorized by an individual in writing

69

Security Rule

- Security rules only applies to e-PHI
- Sets forth administrative, physical, and technical safeguards
  - Safeguards are either required or an alternative may be chosen if justified by explanation

70

Safeguards

- Covered entities must:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

71

Breach Notification Rule

- Requires individuals to be notified if their PHI is involved in a data security breach
- Applies to unencrypted PHI
- Must notify affected individuals

72

Breach

- **Breach** means the acquisition, access use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.
- §164.402

73

HIPAA Enforcement

- After HITECH, companies paid significant monetary fines for failure to comply
- Data breaches of more than 500 people are on the HHS wall of shame

74

Data Breach

- "The HITECH Act defines **data breach** as 'the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.'"

75

Penumbras

- "The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy."
  - 1st – right of association
  - 3rd – prohibition against quartering soldiers
  - 4th – right against unreasonable searches and seizures
  - 5th – right against self incrimination
  - 9th – "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."
- Griswold v. Connecticut, 381 U.S. 479 (1965)

76

Limitations of Government Access

- Whalen provides a judicial recognition that constitutional protection for limited government access about individuals is not limited by explicit constitutional amendments (e.g., the 4th Amendment)

77

From Whalen

- **Decisional privacy** - involves the extent to which a state can become involved with the decisions an individual makes with regard to his/her body and family
- "**Constitutional right to information privacy**" - involves the privacy implications of the collection, use, and disclosure of personal information

78

§1983 Actions

- Constitutional violations in civil law
- Transforms constitutional violations into tort actions and enables plaintiffs to collect damages and obtain injunctions
- Sue state officials instead of the states directly

79

Video Privacy Protection Act (VPPA)

- 18 U.S. Code § 2710 - Wrongful disclosure of video tape rental or sale records

80

Disclosure Liability

- (b)(1) A video tape service provider who knowingly discloses, to any person, **personally identifiable information concerning any consumer** of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

81

Cable Communications Policy Act (CCPA)

- Applies to cable operators and service providers

82

COPPA

- Children's Online Privacy Protection Act of 1998 (COPPA)
- Children's Online Privacy Protection Rule of 2013
- 15 U.S.C. §§6501-6506

83

COPPA Violations

- §6502(a) Acts prohibited (1) In general
- It is unlawful for an operator of a website or **online service directed to children**, or any operator that has **actual knowledge** that it is collecting personal information from a child, **to collect personal information from a child in a manner that violates the regulations** prescribed under subsection (b) of this section.

84

Children under COPPA

- A child under COPPA is a person under the age of 13
  - COPPA is not applicable to children over the age of 13

85

CFAA Penalties

- Obtaining National Security Information Section (a)(1) →10 years
- Accessing a Computer and Obtaining Information Section (a)(2) → 1 or 5 years
- Trespassing in a Government Computer Section (a)(3) → 1 year
- Accessing a Computer to Defraud & Obtain Value Section (a)(4) → 5 years
- Intentionally Damaging by Knowing Transmission Section (a)(5)(A) → 1 or 10 years

86

Protected Computer

- Section 1030(e)(2) defines **protected computer** as:

  a computer—

  (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

  (B) which is used in or affecting interstate or foreign commerce or communication . . . .

87

Telephone Consumer Protections Act (TCPA)

- Do not call lists
- Ability to not received further calls after opting out
- Prohibitions on pre-recorded calls and certain auto dialers
- Prohibitions on unsolicited fax advertisements

88

Spam

- How does the CAN-SPAM Act work?
- FTC Summary
  - http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business

89

CAN SPAM Act

- Prohibits sending deceptive or misleading information and using deceptive subject headings
- Requires inclusion of return addresses in email messages, and
- Prohibits sending emails to a recipient after that recipient has indicated he or she does not wish to receive email messages from the sender

90

Privacy and Substantial State Interest

- "Therefore, the specific privacy interest must be substantial, demonstrating that the state has considered the proper balancing of the benefits and harms of privacy. In sum, privacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it."
- U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999)

91

States/Federal Government Data Breach Laws

- 47 States and D.C. with breach notification laws
  - Need to understand the differences so that the business can comply with the notification requirements

92

Notification to State Agency or Attorney General

- "All the breach notification statutes require notification to the **affected party**. …States that **require notice to a state agency or attorney general** include Alaska, California, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Maryland, Massachusetts, New York, North Carolina, South Carolina, Vermont, and Virginia."

93

Private Right of Action

- Only in a minority of states
- Through a separate statute or under the state's unfair or deceptive trade practices act.

94

Future Risk of Harm=Standing?

- "[A] number of courts have had occasion to decide whether the "risk of future harm" posed by data security breaches confers standing on persons whose information may have been accessed. Most courts have held that such **plaintiffs lack standing because the harm is too speculative**. … Here, no evidence suggests that the data has been—or will ever be—misused. The present test is actuality, not hypothetical speculations concerning the possibility of future injury. Appellants' allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing."
- Reilly v. Ceridian Corp. (3rd. Cir. 2011)

95

Enforcement Actions

- "The FTC's initial **enforcement actions for data security** involved companies that failed to live up to promises made about **data security in their privacy policies**. The FTC has deemed the failure to follow statements made in a privacy policy to be a deceptive act or practice. A deceptive act or practice is a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.'

96

Section 5

- Violation of a consent decree results in fines
- Can issue fines under other sections
- FTC can obtain injunctive relief
- No private right of action

97

FTC v. Wyndham Worldwide Corp.

- Overstated privacy policy
- "The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data."

98

In the Matter of Trendnet

- No more misrepresentations
- Establish and implement a comprehensive security program
- Risk assessments, risk personnel, safeguards, testing and monitoring, etc.
- Notify those affected
- 20 year order

99

Fair Credit Report Act (FCRA)

- "FCRA applies to 'any consumer reporting agency' that furnishes a 'consumer report.' 15 U.S.C. §1681b."

100

US v. Spokeo, Inc.

- "The consumer profiles Spokeo provides to third parties are 'consumer reports' as defined in section 603(d) of the FCRA, 15 U.S.C. §1681a(d). … Section 607(a) of the FCRA, 15 U.S.C. §1681e(a), requires that every consumer reporting agency maintain reasonable procedures to **limit the furnishing of consumer reports** for enumerated 'permissible purposes.' These reasonable procedures include making reasonable efforts to **verify the identity** of each prospective user of consumer report information and the **uses certified by each prospective user** prior to furnishing such user with a consumer report. … Spokeo has failed to maintain such reasonable procedures."

101

Limited Set of "Permissible Purposes"

- "The FCRA identifies a **limited set of "permissible purposes" for obtaining and using a consumer report**. See 15 U.S.C. §1681b(a)(3); see also 15 U.S.C. §1681b(f). Those permissible purposes provide that a person may only access a consumer report if he:
- (A) intends to use the information in connection with a **credit transaction involving the consumer** on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or
- (B) intends to use the information for **employment purposes**; or
- (C) intends to use the information in connection with the **underwriting of insurance** involving the consumer; or

102

Limited Set of "Permissible Purposes"

- (D) intends to use the information in connection with a determination of the consumer's **eligibility for a license** or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or
- (E) intends to use the information, as a **potential investor** or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; or
- (F) otherwise has **a legitimate business need** for the information—
  - (i) in connection with a business transaction that is initiated by the consumer; or
  - (ii) to review an account to determine whether the consumer continues to meet the terms of the account.
- 15 U.S.C. §1681b(a)(3)."

Smith v. Bob Smith Chevrolet, Inc.

103

Legitimate Business Need

- "[N]early every federal court addressing this issue has similarly held that the "**legitimate business need**" permissible purpose should be **narrowly construed** in the context of the other five enumerated purposes …"
- Smith v. Bob Smith Chevrolet, Inc.

104

Sarver v. Experian Information Solutions

- "Section 1681i requires a **credit reporting agency to reinvestigate** items on a credit report when a consumer disputes the validity of those items. An agency can terminate a reinvestigation if it determines the complaint is frivolous, 'including by reason of a failure by a consumer to provide sufficient information to investigate the disputed information.' §1681i(a)(3)."

105

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

106

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 protection and on what basis information is shared;
3. Customers must be given the right, though not absolute, to opt-out of information sharing;

107

GLBA Summary

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

108

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."

109

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. …"

110

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.'"

111

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."

112

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

113

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

114

Telephone Monitoring 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

115

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."

116

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."

117

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].'"

118

Keith Case Framework

1) **Criminal investigations** – warrant required
2) **Domestic national security investigations** – warrant required, but standards need not be the same as for criminal
3) **Foreign intelligence gathering** – not addressed

119

Applicability of FISA

- "FISA generally applies when **foreign intelligence gathering is 'a significant purpose'** of the investigation. 50 U.S.C. §1804(a)(7)(B) and § 1823(a)(7)(B). The language of 'a significant purpose' comes from the USA PATRIOT Act of 2001. Prior to the USA PATRIOT Act, FISA as interpreted by the courts required that the collection of foreign intelligence be the **primary purpose** for surveillance. After the USA PATRIOT Act, foreign intelligence gathering need no longer be the primary purpose."

120

Foreign Intelligence Surveillance Court (FISC)

- "Requests for FISA orders are reviewed by a special court of federal district court judges. … The proceedings are ex parte, with the Department of Justice (DOJ) making the applications to the court on behalf of the CIA and other agencies. The Court meets in secret, and its proceedings are generally not revealed to the public or to the targets of the surveillance."

121

National Security Letters

- "Provisions in several laws permit the FBI to obtain personal information from third parties merely by making a written request in cases involving national security. No court order is required. These requests are called 'National Security Letters' (NSLs)."

122

Snowden Revelations

- NSA

1) "targeting of non-U.S. persons outside the United States through surveillance occurring in the United States (pursuant to Section 702 of FISA);
2) collecting telephone metadata (pursuant to Section 215 of the Patriot Act);
3) spying on foreign countries and their leadership; and
4) acting to weaken encryption standards."

123

Klayman v. Obama

- "[T]he Bulk Telephony Metadata Program is meant to detect: (1) domestic U.S. phone numbers calling *outside* of the U.S. to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers associated with terrorist groups calling *into* the U.S. to U.S. phone numbers; and (3) 'possible terrorist-related communications' between U.S. phone numbers *inside* the U.S. …"

124

Disclosure under FOIA

- Freedom of Information Act
- "OIA grants all persons the **right to inspect and copy records and documents maintained by any federal agency, federal corporation, or federal department**. Certain documents must be disclosed automatically — without anybody explicitly requesting them. FOIA requires disclosure in the Federal Register of descriptions of agency functions, procedures, rules, and policies. 5 U.S.C. §552(a)(1). FOIA also requires that opinions, orders, administrative staff manuals, and other materials be automatically released into the public domain. §552(a)(2)."

125

Agencies under the FOIA

- Only Agencies
- Not Congress and the President and advisors

126

The Privacy Act of 1974

- Stated Purposes include:
- "(1) 'permit an individual to determine what records pertaining to him are **collected, maintained, used, or disseminated by [federal] agencies**'; (2) 'permit an individual to prevent records pertaining to him obtained by such agencies **for a particular purpose from being used or made available for another purpose without his consent**'; (3) allow an individual to **access and correct** his personal data maintained by federal agencies; and (4) ensure that information is '**current and accurate** for its intended use, and that adequate safeguards are provided to **prevent misuse** of such information.'"

127

Applicability of the Privacy Act

- Applies to
  - Federal agencies
- Does not apply to:
  - Businesses or private sector organizations
  - State and local agencies
  - Aspects of the federal government that are not agencies

128

"Routine Use" Exception

- "The broadest exception under the Privacy Act is that information may be disclosed for any '**routine use**' if disclosure is **'compatible' with the purpose** for which the agency collected the information. §552a(b)(3)."

129

"Routine Use" Exception Loophole

- "An agency can establish a 'routine use' if it determines that a disclosure is compatible with the purpose for which the record was collected. This vague formula has not created much of a substantive barrier to external disclosure of personal information…"
- "[M]ore procedural and more symbolic."

130

DNA Profiling

- "Pursuant to the DNA Analysis Backlog Elimination Act of 2000 ('DNA Act'), individuals who have been convicted of certain federal crimes and who are incarcerated, or on parole, probation, or supervised release must provide federal authorities with 'a tissue, fluid, or other bodily sample . . . on which a[n] . . . analysis of the [sample's] deoxyribonucleic acid (DNA) identification information' can be performed. …"
- "[T]he **DNA Act's compulsory profiling** of qualified federal offenders can only be described as **minimally invasive** — both in terms of the bodily intrusion it occasions, and the information it lawfully produces."
- US v. Kincade, 9th Cir. 2004 (en banc)(plurality)

131

Program Completed

132