Privacy and Information Security Law

Randy Canis

CLASS 9

Health Privacy pt. 1; Consumer Data pt. 2
A. CONFIDENTIALITY OF MEDICAL INFORMATION

Oath and Law of Hippocrates

• “Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.”
Evidentiary Privileges

Recognized Privileges

• (1) spousal privilege whereby a person can refuse to testify against his or her spouse in a criminal case; (2) spousal privilege in preventing one’s spouse or former spouse from disclosing marital communications in criminal or civil cases; (3) accountant-client privilege; (4) priest-penitent privilege, whereby a person can prevent the disclosure of confidential communications made when seeking spiritual advice from his or her clergy member; (5) physician-patient privilege; (6) voter privilege, whereby a person can refuse to testify as to how he or she voted in any political election; (7) journalist privilege, where journalists can refuse to divulge information sources; and (8) executive privilege, permitting the President of the United States from divulging secrets necessary to the carrying out of his or her constitutional functions.

Psychotherapist Privilege?

• “[T]he question we address today is whether a privilege protecting confidential communications between a psychotherapist and her patient promotes sufficiently important interests to outweigh the need for probative evidence. . . .” Both “reason and experience” persuade us that it does . . . .
• Jaffe v. Redmond, 518 U.S. 1 (1996)
Cause of Action Against a Physician?

- "The modern trend recognizes that the confidentiality of the physician-patient relationship is an interest worth protecting. A majority of the jurisdictions faced with the issue have recognized a cause of action against a physician for the unauthorized disclosure of confidential information unless the disclosure is compelled by law or is in the patient's interest or the public interest."

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.

Theories for the Cause of Action

- "The jurisdictions that recognize the duty of confidentiality have relied on various theories for the cause of action, including invasion of privacy, breach of implied contract, medical malpractice, and breach of a fiduciary duty or a duty of confidentiality."
Appropriate Disclosure

• "... We conclude, therefore, that ordinarily a physician receives information relating to a patient's health in a confidential capacity and should not disclose such information without the patient's consent, except where the public interest or the private interest of the patient so demands. ..."

• Hammonds v. Aetna Casualty & Surety Co.

Inducement of Breach

• "The law is settled [] that a third party who induces a breach of a trustee's duty of loyalty, or participates in such a breach, or knowingly accepts any benefit from such a breach, becomes directly liable to the aggrieved party. ... [W]hen one induces a doctor to divulge confidential information in violation of that doctor's legal responsibility to his patient, the third party may also be held liable in damages to the patient."

• Hammonds v. Aetna Casualty & Surety Co.

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."
Tarasoff v. Regents of University of California

- **Issue**
  - Does a psychologist owe a duty of care to a potential victim of a patient in the psychologist’s care?

Tarasoff v. Regents of University of California

- “We shall explain that defendant therapists cannot escape liability merely because Tatiana herself was not their patient. When a therapist determines, or pursuant to the standards of his profession should determine, that his patient presents a serious danger of violence to another, he incurs an obligation to use reasonable care to protect the intended victim against such danger. The discharge of this duty may require the therapist to take one or more of various steps, depending upon the nature of the case. Thus it may call for him to warn the intended victim or others likely to apprise the victim of the danger, to notify the police, or to take whatever other steps are reasonably necessary under the circumstances. …”

Tarasoff v. Regents of University of California

- “As a general principle, a defendant owes a duty of care to all persons who are foreseeably endangered by his conduct, with respect to all risks which make the conduct unreasonably dangerous.” … [W]hen the avoidance of foreseeable harm requires a defendant to control the conduct of another person, or to warn of such conduct, the common law has traditionally imposed liability only if the defendant bears some special relationship to the dangerous person or to the potential victim. Since the relationship between a therapist and his patient satisfies this requirement, we need not here decide whether foreseeability alone is sufficient to create a duty to exercise reasonable care to protect a potential victim of another’s conduct.”
Protection of Intended or Potential Victim

• “This 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.”

HIV Notification Statutes

• Some states have partner notification laws
• “According to N.Y. Pub. Health L. § 2130, an HIV-positive diagnosis shall be reported to public health officials. The report “shall include information identifying the protected individual as well as the names, if available, of any contacts of the protected individual … known to the physician or provided to the physician by the infected person.”

Other Disclosure Requirements

• “Many states have statutory requirements for physicians to disclose health information for certain types of diseases or injuries.”
• Collection of certain medical data relating to birth defects, cancer, occupational diseases, infectious diseases, health injuries related to possible child abuse, etc.
State Law Privacy Protections for Medical Information

• Some state regulation of personal information beyond Federal Laws
• “Disclosure of medical information can give rights to a claim for public disclosure of private facts.”
• Certain states have recognized tort liability when physicians disclose a patient’s medical information.

State Law Privacy Protections for Medical Information

• Mandatory report laws – “require that medical personnel or institutions report certain health information to state agencies or to others”
• Research disclosure laws – “regulate the use of medical data for research purposes”
• Medical confidentiality laws – “specific statutes providing civil and criminal protection against the disclosure of medical information”
• Patient access laws – right to access certain medical records

California’s Confidentiality of Medical Information Act

• 56.10. (a) A provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c).
California’s Confidentiality of Medical Information Act

• (c) A provider of health care or a health care service plan may disclose medical information as follows: …
  – (16) The information may be disclosed to a third party for purposes of encoding, encrypting, or otherwise anonymizing data. However, no information so disclosed shall be further disclosed by the recipient in a way that would violate this part, including the unauthorized manipulation of coded or encrypted medical information that reveals individually identifiable medical information.

• (19) The information may be disclosed, consistent with applicable law and standards of ethical conduct, by a psychotherapist, as defined in Section 1010 of the Evidence Code, if the psychotherapist, in good faith, believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

• (d) Except to the extent expressly authorized by a patient, enrollee, or subscriber, or as provided by subdivisions (b) and (c), a provider of health care, health care service plan, contractor, or corporation and its subsidiaries and affiliates shall not intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient.
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

Covered Entities

• “HIPAA regulations apply to health plans, health care clearinghouses, and health care providers.” 45 C.F.R. § 160.102. Health care plans, clearinghouses, and providers that are covered by the regulation are called “covered entities.”

Covered Entities

• A “health care provider” is a “provider of medical or health services … and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.” 45 C.F.R. § 160.103. Examples of health care providers are physicians, hospitals, and pharmacists.
• A “health plan” is “an individual or group plan that provides, or pays the cost of, medical care.” 45 C.F.R. § 160.103. This definition encompasses health insurers and HMOs.
• A “health care clearinghouse” is a public or private entity that processes health information into various formats — either into a standard format or into specialized formats for the needs of specific entities. 45 C.F.R. § 160.103.
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.

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

Business Associate Functions and Activities

• Claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.
Business Associate Services

• Legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial

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

Required Agreement Elements

• Describe the permitted and required uses of PHI by the business associate;
• Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and
• Require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.
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**.

Privacy Officials

- Designed by the company
- Responsible for implementation of privacy policies and procedures
- Designated to receive complaints

Privacy-Related Responsibilities

- Written policies and procedures
- Training for workforce members
- Route assessments of privacy practices
- Appropriate safeguards to protect PHI
Individually Identifiable Health Information

Information relates to:
• the individual’s past, present or future physical or mental health or condition,
• the provision of health care to the individual, or
• the past, present, or future payment for the provision of health care to the individual,
and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual

De-Identified Health Information

• Health information that neither identifies nor provides a reasonable basis to identify an individual
• No restrictions on use or disclosure under HIPAA

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
Authorized Disclosures under the Privacy Rule

1) To the individual
2) For treatment, payment, and health care operations
3) Opportunity to Agree or Object;
4) Incident to an otherwise permitted use and disclosure;
5) Public Interest and Benefit Activities; and
6) Limited Data Set for the purposes of research, public health or health care operations.

Notice of Privacy Practices

• Must include in plain language:
  – How the covered entity may use and disclose an individual’s PHI
  – Individual’s rights with PHI and how individual may exercise these rights
  – Covered entities legal duties with the PHI
  – Whom to contact for further information

HIPAA Marketing

• Marketing under HIPAA
  – a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
• Covered entity generally needs authorization from the individual
Not HIPAA Marketing

- A communication is not “marketing” if it is made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about:
  - The entities participating in a health care provider network or health plan network;
  - Replacement of, or enhancements to, a health plan; and
  - Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

Personal Health Records

- An electronic record of an individual's health information.
- Individual’s rights under the Privacy Rule:
  - Right of access to inspect and obtain a copy of PHI in a designated record held by a covered entity.
  - Right to have corrections or amendments made to PHI in their health records.

Consumer Data pt. 2
F. STATUTORY REGULATION

Basic Areas of Federal Legislation
1) Entertainment records
2) Internet use and communications
3) Marketing

Video Privacy Protection Act (VPPA)
• 18 U.S. Code § 2710 - Wrongful disclosure of video tape rental or sale records
Type of Information Covered

• (a)(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

Video Tape Service Provider

• (a)(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

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).
Written Consent Required for Disclosure

• (b)(2) A video tape service provider may disclose personally identifiable information concerning any consumer— (B) to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that—
  • (i) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;
  • (ii) at the election of the consumer— (I) is given at the time the disclosure is sought; or (II) is given in advance for a set period of time, not to exceed 2 years, or until consent is withdrawn by the consumer, whichever is sooner; and
  • (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer’s election;

Enforcement

(c) Civil Action.—
1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.
2) The court may award— (A) actual damages but not less than liquidated damages in an amount of $2,500; (B) punitive damages; (C) reasonable attorneys’ fees and other litigation costs reasonably incurred; and (D) such other preliminary and equitable relief as the court determines to be appropriate.
3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.
4) No liability shall result from lawful disclosure permitted by this section.

Unique Anonymized IDs

• “[T]he statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person. …”
  • In re Hulu Privacy Litigation
Cable Communications Policy Act (CCPA)

- Applies to cable operators and service providers

Notice

- (a) Notice to subscriber regarding personally identifiable information; definitions
  (1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of—
  - (A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;
  - (B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;
  - (C) the period during which such information will be maintained by the cable operator;
  - (D) the times and place at which the subscriber may have access to such information in accordance with subsection (d) of this section; and
  - (E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.
Written Consent

• (b) Collection of personally identifiable information using cable system
• (1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.
• (2) A cable operator may use the cable system to collect such information in order to— (A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or (B) detect unauthorized reception of cable communications.

Enforcement

• (f) Civil action in United States district court; damages; attorney’s fees and costs; nonexclusive nature of remedy
• (1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.
• (2) The court may award— (A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; (B) punitive damages; and (C) reasonable attorneys’ fees and other litigation costs reasonably incurred.
• (3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

Cable Providers as ISPs

• “[T]he Court should consider the requirements of the Cable Privacy Act, 47 U.S.C. §551. The Act generally prohibits cable operators from disclosing personally identifiable information regarding subscribers without the prior written or electronic consent of the subscriber. 47 U.S.C. §551(c)(1) . A cable operator, however, may disclose such information if the disclosure is made pursuant to a court order and the cable operator provides the subscriber with notice of the order. 47 U.S.C. §551(c)(2)(B). The ISP that Plaintiff intends to subpoena in this case appears to be a cable operator within the meaning of the Act. Providing notice and an opportunity to file a Motion to Quash/Modify gives the ISP and Defendant an opportunity assert any applicable privilege prior to the information being provided to Plaintiff.”
• Rotten Records, Inc. v. John Doe, (W.D.PA 2015)
COPPA

- Children’s Online Privacy Protection Act of 1998 (COPPA)
- Children’s Online Privacy Protection Rule of 2013

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.

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
Do You Collect Personal Information from a Child?

• Website is directed to a Child and you collect PI from them (or let others collect PI from them)
• Website is directed to a general audience, but you have actual knowledge you collect PI from Children
• Ad network or plugin and you have actual knowledge you collect PI from Children

Personal Information

• What PI fall under COPPA?
  – Full name
  – Home or physical address
  – Online contact information including email address
  – Screen or user name
  – Telephone number
  – Social security number
  – Persistent identifiers including cookies and IP address
  – Photos and videos containing a child’s image or voice

Must Post a COPPA compliant Privacy Policy

• Link privacy policy on homepage
• Include
  – List of all operators collecting PI
  – Description of the PI collected and how its used
  – Description of parental rights
Parental Involvement

- Notify parents directly before collecting PI from their kids
- Obtain parental verifiable consent before collecting PI from their kids
- Honor parents ongoing rights by
  - Allow parents to review collected PI
  - Provide a manner to revoke consent
  - Allow for a requested deletion of child’s PI

Electronic Communications Privacy Act (ECPA)

1) Wiretap Act
2) Store Communications Act (SCA)
3) Pen Register Act

Remember?

In re Google, Inc. Gmail Litigation

- Issue
  - Does Gmail violate state and
In re Google, Inc. Gmail Litigation

• “[The] Terms of Service reference Google’s Privacy Policies … [and] stated that Google could collect information that users provided to Google, cookies, log information, user communications to Google, information that users provide to affiliated sites, and the links that a user follows. The Policies listed Google’s provision of ‘services to users, including the display of customized content and advertising’ as one of the reasons for the collection of this information.

In re Google, Inc. Gmail Litigation

• “Plaintiffs who are not Gmail or Google Apps users are not subject to any of Google’s express agreements. Because non-Gmail users exchange emails with Gmail users, however, their communications are nevertheless subject to the alleged interceptions at issue in this case.”

In re Google, Inc. Gmail Litigation

• “[T]he Wiretap Act provides a private right of action against any person who ‘intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.’ 18 U.S.C. §2511(1)(a); see id. §2520 (providing a private right of action for violations of §2511). The Act further defines ‘intercept’ as ‘the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.’”
In re Google, Inc. Gmail Litigation

• “Plaintiffs contend that Google violated the Wiretap Act in its operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising.”

In re Google, Inc. Gmail Litigation

• Defense #1 – “Ordinary Course of Business” Exception
• Exception is narrow…

In re Google, Inc. Gmail Litigation

• “The exception offers protection from liability only where an electronic communication service provider’s interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email.”
In re Google, Inc. Gmail Litigation

• Defense #2 – Consent
  • "The Court rejects Google's contentions with respect to both explicit and implied consent. Rather, the Court finds that it cannot conclude that any party—Gmail users or non-Gmail users—has consented to Google's reading of email for the purposes of creating user profiles or providing targeted advertising."

Computer Fraud and Abuse Act (CFAA)

• Crimes under the CFAA:
  – Knowingly commit espionage by accessing information without authorization or exceeding authorized access;
  – Access other information without authorization or exceeding authorized access;
  – Access any nonpublic government computer;
  – Access any computer with an intent to commit fraud;
  – Knowingly or intentionally damage a computer;
  – Knowingly traffic in passwords;
  – Threaten to cause damage to a computer with the intent to extort money or other things of value

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
CFAA Penalties

- Recklessly Damaging by Intentional Access Section (a)(5)(B) → 1 or 5 years
- Negligently Causing Damage & Loss by Intentional Access Section (a)(5)(C) → 1 year
- Trafficking in Passwords Section (a)(6) → 1 year
- Extortion Involving Computers Section (a)(7) → 5 years

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 . . . .

Insiders v. Outsiders

- Insiders – exceed authorized access
- Outsiders – without authorization
Exceeds Authorized Access

• The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."
• Without authorization is not defined...

Exceeds Authorized Access

• "It is relatively easy to prove that a defendant had only limited authority to access a computer in cases where the defendant's access was limited by restrictions that were memorialized in writing, such as terms of service, a computer access policy, a website notice, or an employment agreement or similar contract."

Obtaining National Security Information

1030(a)(1) Summary (Felony)
1. Knowingly access computer without or in excess of authorization
2. obtain national security information
3. reason to believe the information could injure the U.S. or benefit a foreign nation
4. willful communication, delivery, transmission (or attempt) OR willful retention of the information
Accessing a Computer and Obtaining Information

1030(a)(2) Summary (Misd.)
1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from financial records of financial institution or consumer reporting agency OR the U.S. government OR a protected computer

Accessing a Computer and Obtaining Information

(Felony)
5. committed for commercial advantage or private financial gain OR
committed in furtherance of any criminal or tortious act OR the value of the information obtained exceeds $5,000

Trespassing in a Government Computer

1030(a)(3) Summary (Misd.)
1. Intentionally access
2. without authorization
3. a nonpublic computer of the U.S. that was exclusively for the use of U.S. or was used by or for U.S.
4. affected U.S. use of computer
**Accessing to Defraud and Obtain Value**

**1030(a)(4) Summary (Felony)**
1. Knowingly access a protected computer without or in excess of authorization
2. with intent to defraud
3. access furthered the intended fraud
4. obtained anything of value, including use if value exceeded $5000

**Damaging a Computer or Information**

**Summary of (a)(5)(A)**
1. Knowingly cause transmission of a program, information, code, or command
2. intentionally cause damage to protected computer without authorization

**Summary of (a)(5)(B)**
1. Intentionally access a protected computer without authorization
2. recklessly cause damage
Damaging a Computer or Information

Summary of (a)(5)(C)
1. Intentionally access a protected computer without authorization
2. cause damage
3. cause loss

Felony
3. resulting in loss of $5,000 during 1 year
OR modifies medical care of a person OR causes physical injury OR threatens public health or safety OR damages systems used by or for government entity for administration of justice, national defense, or national security OR damages affect 10 or more protected computers during 1 year

Trafficking in Passwords

1030(a)(6) Summary (Misd.)
1. Trafficking
2. in computer password or similar information
3. knowingly and with intent to defraud
4. trafficking affects interstate or foreign commerce OR computer used by or for U.S.
Threatening to Damage a Computer

1030(a)(7) Summary (Felony)
1. With intent to extort money or any other thing of value
2. transmits in interstate or foreign commerce a communication
3. containing a threat to damage a protected computer OR threat to obtain or reveal confidential information without or in excess of authorization OR demand or request for money or value in relation to damage done in connection with the extortion.

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

Spam

• How does the CAN-SPAM Act work?
• FTC Summary
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

CAN SPAM Act

• Who is subject to the law?
  – Mail service senders
  – Persons provided content to be sent to mail service providers
  – Persons performing their own mailings
  – More than one person can be subject to the law for the sending of a particular email

Commercial Mail Messages

• Is the message a commercial electronic mail message?
  – A “commercial electronic mail message” is any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose);
  – Does not include transactional or relationship messages
Transactional/Relationship Qualifications

• Is the message a transactional or relationship message?
  – The primary purpose of the e-mail must meet a defined category
  – Effectuate a transaction, product/service related information for the already purchased product/service, notification of changes, account information (on a regular basis), employment relationship/benefit information, or deliver agreed upon goods/services

Transactional/Relationship Qualifications

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;
(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide—
  (I) notification concerning a change in the terms or features of;
  (II) notification of a change in the recipient’s standing or status with respect to; or
  (III) at regular periodic intervals, account balance information or other type of account statement with respect to,
  a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;
Transactional/Relationship Qualifications

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

Transactional or Relationship?

• If you don’t fit in the bucket of being a transactional or relationship message,
  – Either your message is a commercial electronic mail message and you have the associated enhanced obligations, or
  – Your message does not fall within the purview of the CAN SPAM Act.

False or misleading header information

• For commercial electronic mail, transactional, and relationship mail messages
• When email address or domain name is obtained under false pretenses
• When origin of message is disguised due to relay
• Not when from line accurately identifies who initiated the message
Deceptive Subject Heading

- Applies only to commercial electronic mail messages
- Cannot have a subject line that would be likely to mislead the recipient about a material fact about the contents or subject matter of the message

Return Email Address

- Applies only to commercial electronic mail messages
- Must have a functioning return email address that works for 30 days after transmission
- Alternatively, the message can provide another Internet mechanism to enable opt-out
  - Can provide a menu of options, so long as menu enables opt out of all commercial electronic mail messages from the sender
- Must remove person within 10 business days

Opt Out and Physical Address

- Applies only to commercial electronic mail messages
- Message must have
  (i) clear and conspicuous identification that the message is an advertisement or solicitation;
  (ii) clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender; and
  (iii) a valid physical postal address of the sender.
CAN SPAM Rule

- The rule "defines the relevant criteria to determine the primary purpose of an electronic mail message. [The] provisions [of this rule] describe types of electronic mail messages that contain commercial content or what the Act terms 'transactional or relationship' content, and establish different criteria for each type."

Primary Purpose

- Commercial when
  - Content is exclusively commercial
  - If content is both commercial and transactional/relational, then when:
    • Subject line reflects that the message is commercial, or
    • Transactional or relationship content (or other content) does not substantially appear at the beginning of the message

Program Completed

All course materials - Copyright 2015 Randy L. Canis, Esq.