Legal Environment

Randy Canis

CLASS 14

Environmental Law; Constitutional Authority; Consumer Law; Securities Law; HI PAA; DMCA
Environmental Law

Nuisance

- May be held liable if property is used in a manner that unreasonable interferes with others’ rights to use or enjoy their property
- Balance the hardship caused by pollution against the cost of stopping it

Negligence and Strict Liability

- May be held liable in tort law under negligence and strict liability for failure to use reasonable care toward a party whose injury was foreseeable and was cause by the lack of reasonable care
State and Local Regulations

- State laws
  - Regulate discharge of chemicals into the air, disposal and recycling of waste, and vehicle emissions
- Local laws
  - Zoning laws
  - Regulate waste removal, building appearance, and maximum noise level

Federal Regulations

- Federal statutes are generally designed to address pollution in the air, water, or land

Rivers and Harbors Appropriations Act

- To prohibit ships and manufacturers from discharging and depositing refuse in navigable waterways
- 33 USC 401-418
Federal Insecticide, Fungicide, and Rodenticide Act
- To control use of pesticides and herbicides
- 7 USC 146-136y

Clean Water Act
- To eliminate the discharge of pollutants from major sources into navigable waters
- Goals
  - Make waters safe for swimming
  - Protect fish and wildlife
  - Eliminate the discharge of pollutants in the air
- 33 USC 1251-1387

Clean Air Act
- To control air pollution from mobile and stationary sources
  - Mobile – specified pollution standards and time schedules for meeting the standards
  - Stationary – primary responsibility is with state and local government; aimed and controlling hazardous pollutants
- 42 USC 7401-7671q
National Environmental Policy Act

- To limit environmental harm from federal government activities
- 42 USC 4321-4370d
- Requires an environmental impact statement (EIS) for every major federal action that significantly affects the quality of the environment

Environmental Impact Statement (EIS)

- Must analyze:
  1. The impact on the environment that the action will have,
  2. Any adverse effects on the environment and alternative actions that might be taken, and
  3. Irreversible effects the action might generate

Ocean Dumping Act

- To prohibit the dumping of radiological, chemical, and biological warfare agents and high-level radioactive waste into the ocean
- 16 USC 1401-1445
Endangered Species Act

- To protect species that are threatened with extinction
- 16 USC 1531-1544

Safe Drinking Water Act

- To regulate pollutants in public drinking water systems
- Sets maximum level of pollutants in the public water systems
- 42 USC 300f-300j-25

Resource Conservation and Recovery Act

- To establish standards for hazardous waste disposal
- 42 USC 6901-6986
Toxic Substances Control Act
- To regulate toxic chemicals and chemical compounds
- 15 USC 2601-2692

Comprehensive Environmental Response, Compensation, and Liability Act
- To regulate the clean-up of hazardous waste-disposal sites
- 42 USC 9601-9675

Oil Pollution Act
- To establish liability for the clean-up of navigable waters after oil-spill disasters
- 33 USC 2701-2761
Small Business Liability Relief and Brownfields Revitalization Act

- To allow developers who comply with state voluntary clean-up programs to avoid federal liability for the properties that they decontaminate and develop
- 42 USC 9628

Who Can Sue?

- If the governmental fails to sue for a violation of an environmental law, citizens can typically sue if they meet the standing requirement to sue

Constitutional Authority
Federal Form of Government

- National government and the states share sovereign power
- Specific powers set forth by Constitution
- Implied powers to undertake actions necessary to carry out expressly designated powers

Powers of the States

- State governments have the authority to regulate affairs within their borders
- 10th Amendment – reserves all powers not delegated to the national government to the states or the people.
- Police Powers – broad right of states governments to regulate private activities to protect or promote the public order, health, safety, morals, and general welfare.

Judicial Review

- Courts have the final say on the constitutionality of law
  - “It is emphatically the province and duty of the judicial department to say what the law is. Those who apply the rule to particular cases, must of necessity expound and interpret that rule. If two laws conflict with each other, the courts must decide on the operation of each.”
- Part of the constitution?
Privileges and Immunities Clause

• Article IV, Section 2 of the Constitution
• Prevent unreasonable burdens on citizens of another state

Full Faith and Credit Clause

• Article IV, Section 1
• Civil matters
• Rights established under deeds, wills, contracts, and similar instruments in one state will be honored in other states.

Commerce Clause

• Congress regulates commerce:
  – Foreign nations
  – Among the several states
  – With the Indian tribes
  – Within the states so long as the commerce substantially affects commerce involving more than one state
Supremacy Clause

• The Constitution, laws, and treaties of the US are the supreme law of the land
• Conflict between state and federal law—federal law governs.
• However, some powers are concurrent

Preemption

• A valid federal statute or regulation will take precedence over a conflicting state or local law or regulation on the same general subject.

Bill of Rights

• Series of protections for the individual against various types of interference by the federal government
Freedom of Speech

- Expression is subject to reasonable restrictions
- Is the restriction content neutral?
  - Restriction must be aimed at combating some societal problem and not be aimed at suppressing the expressive conduct or its message.

Commercial Speech

- Expression that either:
  1) is related to the economic interest of the speaker and its audience
  2) proposes a commercial transaction

Commercial Speech

- Government may regulate when:
  1) Substantial government interest to justify the regulation
  2) Must directly advance the interest
  3) Must go no further than necessary to accomplish the objective
Obscene Speech

- First amendment does not protect obscene speech
- Material is obscene if
  - The average person finds that it violates contemporary community standards,
  - The work taken as a whole appeals to a prurient (arousing or obsessive) interest in sex;
  - The work shows patently offensive sexual conduct;
  - The work lacks serious redeeming literary, artistic, political, or scientific merit

Reno v. ACLU

- Issue: At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet.
- Holding: Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, we agree with the three judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment.

Freedom of Religion

- Establishment clause – government may not establish any religion
- Free exercise clause – government may not prohibit the free exercise of religious practices
Searches and Seizures

- Law enforcement officers must usually obtain a search warrant to authorize a search or seizure
  - Must have probable cause
  - Must have a particular description of what is to be searched or seized

5th Amendment

- Accused person cannot be forced to give testimony that might subject him or her to any criminal prosecution
- Only natural people, not corporations

Procedural Due Process

- Government must give notice and an opportunity to be heard before an impartial, neutral decision maker before taking life, liberty, or property
Substantive Due Process

• Legislation must be fair and reasonable in content and must further limit a government objective
• If a fundamental right is limited, the state must have a legitimate and compelling interest to justify its action

Equal Protection

• The government cannot enact laws that treat similarly situated individuals differently
• Classes of people cannot be treated differently on an arbitrary basis

Levels of Scrutiny

• Strict scrutiny – basis for distinction must be necessary to promote a compelling state interest
• Intermediate scrutiny – basis for distinction must be substantially related to important government objectives
• Rational basis – basis for distinction must have a conceivable rational basis
Consumer Law

False/Deceptive Advertising

• Occurs if a reasonable consumer would be misled by the advertising claim
  1) There must be a representation, omission, or practice that is likely to mislead a consumer
  2) The act or practice must be considered from the perspective of a consumer that is acting reasonably
  3) The representation, omission, or practice must be material

Bait-and-Switch Advertising

• Advertising a low price for a particular item that will likely be unavailable to the consumer, who will then be encouraged to purchase a more expensive item
• Per FTC guidelines, occurs when:
  – Refuses to show
  – Fails to promise to deliver the advertised item within a reasonable time
  – Discourages employees from selling the item
Online Deceptive Advertising

- FTC guidelines:
  - All ads must be truthful and not misleading
  - Claims made in ad must be substantiated
  - Ads cannot be unfair
  - Clear and conspicuous disclosure of any qualifying or limiting information

FTC Tools and Remedies

1. Guides on how advertising can be performed in certain industries
2. Voluntarily agreement to terminate the advertisement and not use the claim again
3. Consent agreement to terminate the advertisement and not use the claim again
4. Litigated order before ALJ, can be appealed to Fed Court
5. FTC may ask for substantiation
6. FTC may require corrective advertising
7. FTC can seek injunctions
8. FTC can issue trade regulation rules

Labeling and Packaging Laws

- Multiple state and federal laws for various products
  - Tobacco – warnings
  - Cars – EPA fuel economy estimate
  - Food – product labels must identify (1) the product; (2) the net quantity of the contents and serving size, (3) the manufacturer, (4) the packager or distributor + where food originated
Sales

- Door-to-door – right of purchaser to cancel within 3 business days
- Mail order – ship orders within the time promised in their catalogues or advertisements and to notify when cannot be shipped on time
  - Unsolicited merchandise can be kept, thrown away, or disposed of without obligation to sender

Securities Law

Functions of the SEC

- Interprets federal securities laws and investigates security law violations
- Issues new rules and amends existing rules
- Oversees the inspection of securities firms, brokers, investment advisers, and rating agencies
- Oversees private regulatory organizations in the securities, accounting, and auditing fields
- Coordinates U.S. securities regulation with federal, state, and foreign authorities
Acts

- **1933 Act** – initial sales of stock for businesses
- **1934 Act** – regulation and registration of securities exchanges, brokers, dealers, and notional securities associations; continuous periodic disclosures required by publicly held corporations to enable the SEC to regulate subsequent trading

What is a Security?

- Instruments and interests commonly known as securities including stocks, bonds, debentures, and stock warrants
- Interests known as securities including stock options, puts, calls
- Notes, instruments, or other evidence of indebtedness
- Any fractional undivided interest in oil, gas, or other mineral rights
- Investment contracts

Registration

- If a security does not qualify for an exception, it must be registered before it is offered to the public
SEC Rule 10b-5

- Covers about any form of security
- Covers almost all cases concerning trading of securities
- Major goal is to prevent insider trading

Insider Trading

- Persons buy or sell securities on the basis of information that is not available to the public
- Liability extended to those who take advantage of information in their personal transactions

Enforcement Actions

- The SEC regularly brings insider trading enforcement actions against:
  - Corporate officers, directors, and employees who traded the corporation's securities after learning of significant, confidential corporate developments.
  - Friends, business associates, family members, and other "tippees" of such officers, directors, and employees, who traded the securities after receiving such information.
  - Other persons who misappropriated, and took advantage of, confidential information from their employers.
**Ponzi Scheme**

- “A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organizers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. With little or no legitimate earnings, Ponzi schemes require a constant flow of money from new investors to continue. Ponzi schemes inevitably collapse, most often when it becomes difficult to recruit new investors or when a large number of investors ask for their funds to be returned.”

**Disclosure Under Rule 10b-5**

- Any material omission or misrepresentation of material facts in connection with the purchase or sale of a security may violate
- Key is materiality
  - Would it be likely to affect an investor’s decision as to whether to purchase or sell the company’s securities?

**Forward-Looking Statements**

- PSLRA has a safe harbor for forward-looking statements including financial forecasts
- Forward-looking statements must be accompanied by meaningful cautionary statements
Tipper/Tippee Theory

- Anyone who acquires inside information as a result of a corporate insider's breach of his/her fiduciary duty can be liable under SEC Rule 10b-5

Misappropriation Theory

- An individual who wrongfully obtains inside information and trades on it for his/her personal gain is liable because the individual stole information rightfully belonging to another

Blue Sky Laws

- Laws that regulate the offer and sale of securities within the borders of a state
Stock Options

- Enables certain company employees to purchase shares of the corporation’s stock at a set price.
- Assuming the options have vested and the stock has risen from the price at the time of the offering, the employees can sell their shares for a profit.

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."

- 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.

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

- Designated 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
- Routine 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 disclosure 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
Security Rule Basics

• “The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called ‘covered entities’ must put in place to secure individuals’ ‘electronic protected health information’ (e-PHI).”

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

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

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
Defined Security Measures?

- "When a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:
  - Its size, complexity, and capabilities,
  - Its technical, hardware, and software infrastructure,
  - The costs of security measures, and
  - The likelihood and possible impact of potential risks to e-PHI

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

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
Breach Exclusions

- Certain unintentional acquisitions, accesses, or uses of PHI by a workforce member or person acting under the authority of a covered entity or a business associate
- Inadvertent disclosures by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate
- A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- §164.402

Enforcement and Preemption

- Civil penalties – fines of 50K-1.5 million per provision of HIPAA violated
- Criminal penalties – with a malicious motive, personal fines of up to 250K and up to 10 years in jail
- No private right of action
- States can pass more stringent requirements

HIPAA Complaints

- Most investigated complaints:
  1. Impermissible uses and disclosures of protected health information;
  2. Lack of safeguards of protected health information;
  3. Lack of patient access to their protected health information;
  4. Uses or disclosures of more than the minimum necessary protected health information; and
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

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.’"
DMCA

- The DMCA is the Digital Millennium Copyright Act that was signed into law on October 28, 1998.
- The DMCA amended and augmented parts of the existing Copyright Act (i.e., Title 17).

Sony v. GameMasters

- "The Digital Millennium Copyright Act, among other things, prohibits distribution of any product or device which:
  1) is primarily designed or produced for the purpose of circumventing a technological measure (or a protection afforded by a technological measure) that effectively controls access to a system protected by a registered copyright or effectively protects a right of a copyright owner in a registered work or portion thereof;
  2) has only limited commercially significant purpose or use other than to circumvent such a technological measure (or protection afforded it); Or
  3) is marketed for use in circumventing such a technological measure (or protection afforded by it). 17 U.S.C. §§ 1201(a)(2)-(3) and (b)(1)-(2) (Public Law 105-304, October 28, 1998)."

Sony v. GameMasters

- "Section 1201 also prohibits manufacture or distribution of technologies, products and services used to circumvent technological measures which control access. The prohibition applies only if such circumventing technologies are primarily designed for this purpose, have only limited commercial purpose beyond such circumventing purpose, or are marketed for the prohibited purpose. This provision is immediately effective. …"
Universal Studios v. Reimerdes

• The DMCA contains two principal anticircumvention provisions.
• The first, Section 1201(a)(1), governs "[t]he act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work," an act described by Congress as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book."
• The second, Section 1201(a)(2), which is the focus of this case, "supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies developed or advertised to defeat technological protections against unauthorized access to a work."
• As defendants are accused here only of posting and linking to other sites posting DeCSS, and not of using it themselves to bypass plaintiffs' access controls, it is principally the second of the anticircumvention provisions that is at issue in this case.

Universal Studios v. Reimerdes

• "The Court begins its statutory analysis, as it must, with the language of the statute... Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are "not ... infringement[s] of copyright." Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate."

DMCA Rulemaking

• DMCA Rulemaking has established exemptions since 2000; last one was in 2015
• Rule makings conducted
  – http://copyright.gov/1201/
• Current rulemaking (2015) is located here:
ISPs and the DMCA

• Internet Service Providers (ISPs) are concerned with their liability for subscribers who use their resources to commit unlawful acts. The greatest concern has been liability for copyright infringement, as their users transmit a vast amount of material through the Internet and it is impractical to screen out infringing material. The law was unprepared for the wealth and speed of material available on the Internet and, as a result, legal reform was necessary to protect ISPs from liability from actions taken by their subscribers.

ISPs and the DMCA

• Congress responded to the plight of ISPs by introducing legislation that would provide them with "safe harbors" (i.e., exemptions) that would shield them from liability in certain circumstances. In 1998, the Online Copyright Infringement Liability Limitation Act (OCILLA) was signed into law as part of the Digital Millennium Copyright Act and provided safe harbors to protect ISPs in four distinct circumstances: (a) transitory digital network communications, (b) system caching, (c) information residing on systems or networks at direction of users, and (d) information location tools. OCILLA was written into law as 17 U.S.C. §512.

Summary of the Safe Harbors

• OCILLA provides safe harbors to ISPs in four distinct circumstances: transitory digital network communications (i.e., 512(a)), system caching (i.e., 512(b)), information residing on systems or networks at direction of users (i.e., 512(c)), and information location tools (i.e., 512(d)). It is not necessary to obtain all four safe harbors to avoid liability.
• Rather, when the behavior of an ISP falls within a particular safe harbor, that behavior will be exempted harbor if the ISP meets the prerequisites for obtaining the safe harbor as well as the particular requirements of the specific safe harbor.
Program Completed

All course materials © Copyright 2000-16 Randy L. Canis, Esq.