INTERNET Law  
  
a Law school outline *by* corbin dodge  
  
Got Outlines?   
 [corbin-dodge.com](http://www.corbin-dodge.com)  
  
Fall 2014 | Professor Ng | South TX College of Law

Table of Contents

Tips 3

ABOUT THIS OUTLINE 4

Syllabus 5

Internet Jurisdiction p. 465-479 6

Computer Crime 7

Computer Fraud and Abuse Act (CFAA) 7

Computer Fraud and Abuse Act (EFAA) 7

Identity Theft 10

Identity Theft and Assumption Deterrence Act 10

Notification of Identity Theft 10

Spam 10

CAN-SPAM Act of 2003 10

Spam 11

Phishing and Botnets 11

Music and Software Piracy 11

Criminal Policy 11

No Electronic Theft Act 11

Theft of Proprietary Economic Info and Trade Secrets 12

Economic Espionage Act of 1996 (EEA) 12

Evidence 12

Search & Seizure 12

PRIVACY 13

(Missed Class 9/9 Absence #1) 13

Government Collection and Disclosure of Personal Information 13

Controlled Substances 13

Interception of Communications 13

Restricting Use by the Gov’t of Information in Gov’t Records 13

Counterintelligence Access to Telephone Toll and Transactional Records 13

Stored Communications Act (SCA) 13

Private Collection and Disclosure of Information 13

Federal Wiretap Act 13

Electronic Communications & Privacy Act (ECPA) 13

Children’s Online Privacy Protection Act (COPPA) 14

Privacy of Internet Users 14

Digital Millennium Copyright Act 14

Right to Accuracy of Information, 713-735 15

Section 1.01 Databanks 15

REGULATion of INTERNET CONTENT, 737-781 16

Social Media – Defamation & Disparagement 16

Internet Discriminatory Advertising 16

Pornography and Indecency 16

Public Libraries 16

Intellectual Property Rights vs. Free Speech 16

Domain Names 16

Anonymous and Pseudonymous communications 16

Encryption Software and the First Amendment 17

Cyberbullying 17

Anti- Strategic lawsuit against public participation (Anti-SLAPP) 17

ELECTRONIC TRANSACTIONS (481-512) 18

Old and New Situations 18

Paper Transactions 18

Authentication of Signatures 18

Electronic Signatures in Global and National Commerce Act (The ESIGN Act) 18

Uniform Electronic Transactions Act (UETA) 19

Computer Fraud and Abuse Act 20

Bankruptcy-Protecting Software Users 20

Consumer Protection by the FTC 20

Communications Decency Act 20

Taxations 21

Restricting E-Competition 21

Unlawful Internet Gambling Enforcement Act 21

US – Measure Affecting the Cross-Border Supply of Gambling and Betting Services 21

TELECOMMUNICATIONS and the Internet 22

Telecommunications Act of 1996 22

Regulation of Internet Service Providers 22

IP-Enabled Communications 22

Carrier Traffic Management & Network Neutrality 22

Cloud Services 22

TRADEMARK 23

Discipline 23

Lanham Act 23

Confusion 23

Federal Trademark Dilution Act 24

Anti-Cybersquatting Consumer Protection Act 24

Domain Name Dispute Resolution 24

Uniform Domain Name Dispute Resolution Policy (UDRP) *(primary)* 25

Uniform Rapid Suspension (URS) *(new, not utilized yet)* 25

Defenses 25

Nominative Fair Use 25

Functional Use 25

Unfair Business Practices – unsolicited email 26

COPYRIGHT (1-186) 27

Fair Use 27

Liability & Torts 28

Trespass to Chattels 28

Intentional trespass 28

iCANN-SPAM – pre-empts state anti-spam laws 28

Defamation 28

Misappropriation 28

Electronic Communications Privacy Act of 1986 (ECPA) 29

Computer Fraud and Abuse Act (CFAA) 29

Texas Identity Theft Enforcement and Protection Act 30

Tips

* **Room:** 514 **Contact Info:**
* **Exam Format**
  + Typically MC + Essay
  + Fall 2014 semester was a take-home test w/ 6 essays. Since it was a take-home exam, the exam was longer, requiring 6-8 hours of work to complete.
* **Do:** Participate. He likes participation.
* **Don’t:**
* **Notes:**
  + He refers to all malware as a virus. A trivial difference but can be misleading *see my notes on the article* [*Viruses, Spyware, and Malware: What’s the Difference*](https://www.evernote.com/l/ASzntpuxtKdENab5fv32ZknVcnpnBMyrEiY)
  + Bring in recent tech news to discuss at the beginning of each class
  + **The rules he recites**
    - Rule #1 Do what you say you’re going to do
    - Rule #2 Take care of people, take care of you

# ABOUT THIS OUTLINE

**A Note About this Outline**

* My outlines utilize the ‘Styles’ feature in Microsoft Word. An investment of your time in learning how to use the styles feature will allow you to use some of Microsoft Words most powerful features. But be warned, styles can be tricky. The styles that are used in this document are demonstrated below. The Table of Contents can be dynamically updated because it is based on these styles. To learn more about the benefits of using styles, as well as tips and tricks, visit\_\_\_\_\_. For more outlines, visit [www.corbin-dodge.com](http://www.corbin-dodge.com).

**FAQs**

* **How do I apply a different font to any style?**   
  On the main menu, select Format/Style. Highlight the style that you would like to modify. Select modify. Choose your font. Make sure that the option to “Automatically update style” is not checked. Click Apply.
* **How do I update the Table of Contents?**
* Right-click and select “Update Field.” Choose the option to update all page numbers.

H1 (optimized for Helvetica, 16 pt)

H2

* **List paragraph (+Bold) (Optimized for Helvetica 9pt)**
  + List paragraph
    - List paragraph (+ indent)
      * List paragraph (+ indent)
        + etc.

H3

* **List paragraph (+Bold)**
  + List paragraph
    - List paragraph (+ indent)
      * List paragraph (+ indent)
        + etc.

# Syllabus

**Objective:** This course provides students the substantive law regulating Internet and electronic commerce in a comprehensive manner. This course also allows students to consider ethical and professional questions related to the subject matter.

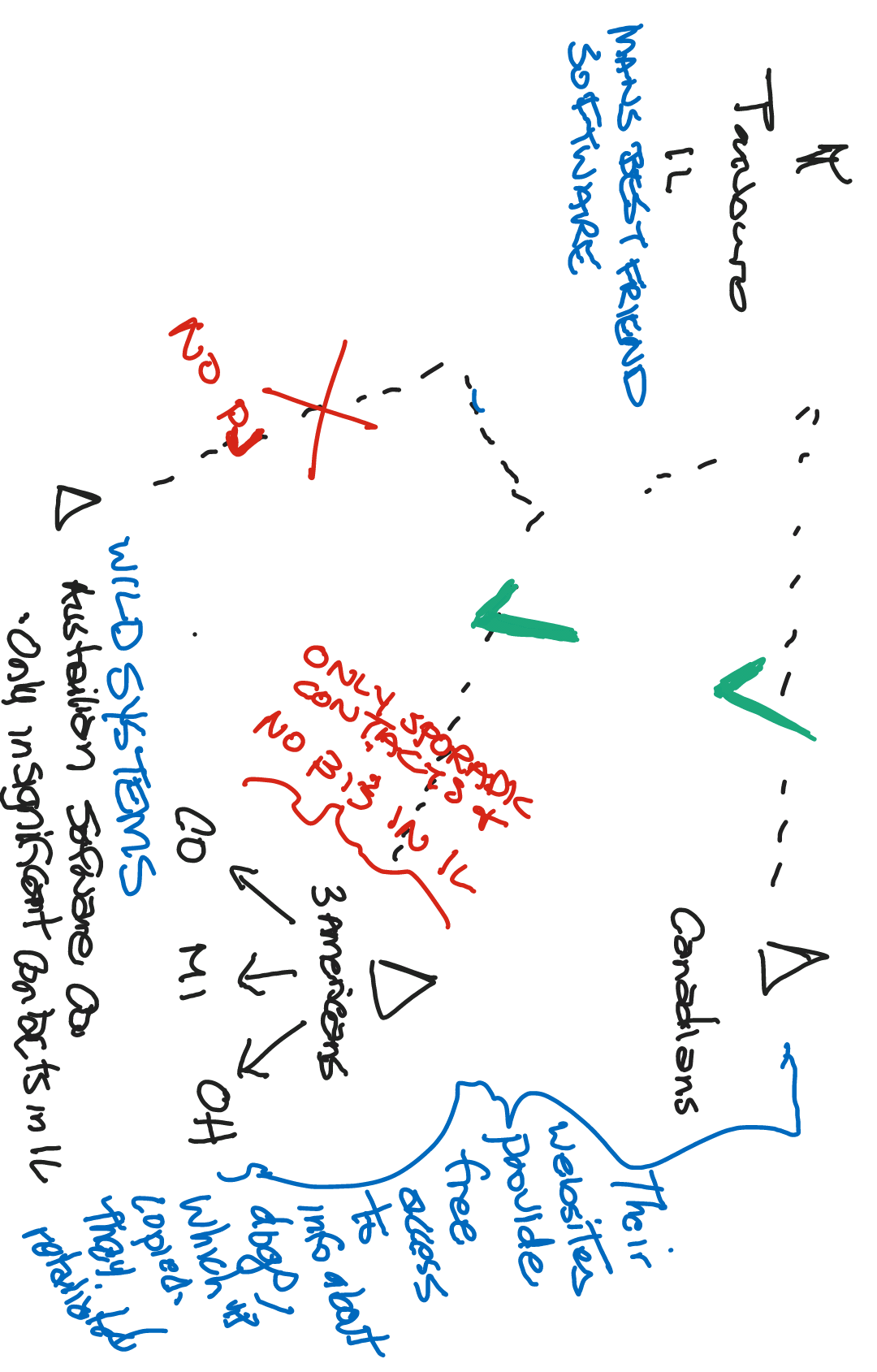
**Class Time:** Tuesday 2:30 – 4:30 p.m.

**Office Hours:** By appointment

**Text:** Internet and Computer Law, 4th ed., Peter B. Maggs and John T. Soma

**Grading:** There will be one final exam. The final exam will have both multiple choice and essay questions. Students who are well prepared and participate in class are eligible for grade enhancement.

# Internet Jurisdiction p. 465-479

* In order for a Ct to exercise jurisdiction over a person or entity, it must have **Subject Matter Jurisdiction** over the controversy
* First, is there jurisdiction under state law, including state “long-arm” statutes?
* Does the ∆ have such *“continuous and systematic contacts* w/ the forum state such as to justify the Cts exercise of *general jurisdiction?*
* Did the ∆ *purposefully avail* himself of the forum?
* Second, is the exercise of this jurisdiction constitutional *(does not violate fair play & substantial justice)*?
* **Personal Jurisdiction**
  + **Long arm statutes** – reach the ∆ in another state.
    - **2 types:**
      * a) 14th amendment
      * b) Minimum contacts – How active ∆ in the state?
    - **General Jurisdiction** ∆/Forum Requires that the ∆ have certain minimum contacts w/ the forum state
    - **Specific Jurisdiction**  ∆/Forum/Litigation ∆ must have *purposefully availed* himself of the forum
  + **TX**
    - A little different from other cases
    - We still use a sliding scale test. Or something.
    - Most states use more traditional min contacts stuff as well. But not on test
  + 
* **Forum Selection/ Arbitration Clauses** – big company usually wins, as these clauses are usually upheld.
* ***uBid, Inc. V. The GoDaddy Group, Inc.***
* ***In Rem* Jurisdiction Over Domain Names**
* ***Office Depot, Inc. v. Zuccarini***– Domain Names are located in the forum state of the registry for the purpose of asserting *quasi In Rem Jurisdiction*
* So not necessarily
* *In Rem* suit over a claim to oproperty
* *Quasi in Rem* b/c intangible

# Computer Crime

Computer Fraud and Abuse Act (CFAA)

Computer Fraud and Abuse Act (EFAA)

* **Purpose 18 U.S.C. § 1030;** [Wikipedia](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act)
  + Amended existing computer fraud law, which had been included in the [Comprehensive Crime Control Act of 1984](http://en.wikipedia.org/wiki/Comprehensive_Crime_Control_Act_of_1984)
  + Clarified and increased the scope of the previous law while
  + But limited federal jurisdiction to cases "with a compelling federal interest
    - i.e., where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature." (see "Protected Computer", below).
  + Criminalized additional computer-related acts
    - Distribution of malicious code
    - Denial of service attacks
    - Trafficking in passwords
* **Protected Computers**
  + CFAA only covers protected computers
  + **Definition:** A computer: [**18 U.S.C. § 1030(e)(2)**](http://www.law.cornell.edu/uscode/18/1030(e)(2).html)
    - exclusively for the use of a financial institution or the US Government, or any computer, when the conduct constituting the offense affects the computer's use by or for the financial institution or the Government; **or**
    - which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the US that is used in a manner that affects interstate or foreign commerce or communication of the US.
  + **Includes**: Any ordinary computer,including cellphones, due to the inter-state nature of most internet communication
* **Criminal Offenses**
  + (a) Whoever—
    - **Computer Espionage. Based on** [**Espionage Act of 1917**](http://en.wikipedia.org/wiki/Espionage_Act_of_1917)**, w/ notable addition that it also covers information related to "Foreign Relations" (not simply "National Defense" like the Espionage Act)**   
      (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of s§ 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
    - ***See also* Conspiracy to violate (a) 18 U.S.C. § 1030(b)**
    - **Computer trespassing, and taking gov’t, financial, or commerce info** (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
      * (A) information contained in a financial record of a financial institution, or of a card issuer as defined in 15 U.S.C. § 1602(n), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
      * (B) information from any department or agency of the US; or
      * (C) information from any protected computer;
    - **Computer trespassing in a gov’t computer**
    - (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
    - **Committing fraud with computer**
    - (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
  + **Damaging a protected computer (including viruses, worms)**
  + (5)
    - (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
    - (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
    - (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.
  + **Trafficking in passwords of a government or commerce computer**
  + (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
    - (A) such trafficking affects interstate or foreign commerce; or
    - (B) such computer is used by or for the Government of the United States;
  + **Threatening to damage a protected computer**
  + (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
    - (A) threat to cause damage to a protected computer;
    - (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
  + (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion
* **Penalties 18 U.S.C. § 1030(c)**
* **2008 Amendments**
  + Eliminated the requirement that information must have been stolen through an interstate or foreign communication, thereby expanding jurisdiction for cases involving theft of information from computers;
  + Eliminated the requirement that the defendant’s action must result in a loss exceeding $5,000 and created a felony offense where the damage affects ten or more computers, closing a gap in the law;
  + Expanded (a)(7) to criminalize not only explicit threats to cause damage to a computer, but also threats to (1) steal data on a victim's computer, (2) publicly disclose stolen data, or (3) not repair damage the offender already caused to the computer;
  + Created a criminal offense for conspiring to commit a computer hacking offense under § 1030;
  + Broadened the definition of “protected computer” in [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 1030(e)(2)](http://www.law.cornell.edu/uscode/18/1030(e)(2).html) to the full extent of Congress’s commerce power by including those computers used in or affecting interstate or foreign commerce or communication; and
  + Provided a mechanism for civil and criminal forfeiture of property used in or derived from § 1030 violations
  + Amended in 2002 by the [USA PATRIOT Act](http://en.wikipedia.org/wiki/USA_PATRIOT_Act)
  + Amended in 2008 by the Identity Theft Enforcement and Restitution Act
* **Case Law**
  + [*United States v. Riggs*](http://en.wikipedia.org/wiki/United_States_v._Riggs), brought against people associated with [*Phrack*](http://en.wikipedia.org/wiki/Phrack) magazine for obtaining a document (known as the "E911 document") about information on BellSouth products implementing 911 emergency telephone services, a case described in [Bruce Sterling](http://en.wikipedia.org/wiki/Bruce_Sterling)'s "Hacker Crackdown of 1990". The government dropped the case after it was revealed that the document was on sale by [AT&T](http://en.wikipedia.org/wiki/AT%26T) for $13.
  + [*United States v. Morris (1991)*](http://en.wikipedia.org/wiki/United_States_v._Morris_(1991)), 928 F.2d 504, decided March 7, 1991. After the release of the [Morris worm](http://en.wikipedia.org/wiki/Morris_worm), an early [computer worm](http://en.wikipedia.org/wiki/Computer_worm), its creator was convicted under the Act for causing damage and gaining unauthorized access to "federal interest" computers. The Act was amended in 1996, in part, to clarify language whose meaning was disputed in the case.[[3]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-usvmorris505-3)
  + *Theofel v. Farey Jones*, 2003 U.S. App. Lexis 17963, decided August 28, 2003 (U.S. Court of Appeals for the Ninth Circuit), holding that the use of a civil subpoena which is "patently unlawful," "in bad faith," or "at least gross negligence" to gain access to stored email is a breach of both the CFAA and the [Stored Communications Act](http://en.wikipedia.org/wiki/Stored_Communications_Act).
    - CFAA doesn’t require a showing that ∆ intentionally prevented authorized use and thereby caused loss *US v Morris*
  + [*International Airport Centers, L.L.C. v. Citrin*](http://en.wikipedia.org/wiki/International_Airport_Centers,_L.L.C._v._Citrin), 2006, [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 1030(a)(5)(A)(i)](http://www.law.cornell.edu/uscode/18/1030.html#a_5_A_i), in which Jacob Citrin [deleted files](http://en.wikipedia.org/wiki/Data_erasure) from his company computer before he quit, in order to conceal alleged bad behavior while he was an employee.
  + [*LVRC Holdings v. Brekka*](http://en.wikipedia.org/wiki/LVRC_Holdings_v._Brekka), 2009 1030(a)(2), 1030(a)(4), in which LVRC sued Brekka for allegedly taking information about clients and using it to start his own competing business.
  + [*Robbins v. Lower Merion School District*](http://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District) (U.S. Eastern District of Pennsylvania), where plaintiffs charged two suburban Philadelphia high schools secretly spied on students by surreptitiously and remotely activating webcams embedded in school-issued laptops the students were using at home, violating the Act. The schools admitted to secretly snapping over 66,000 webshots and screenshots, including webcam shots of students in their bedrooms.
  + [*United States v. Lori Drew*](http://en.wikipedia.org/wiki/United_States_v._Lori_Drew), 2008. The [cyberbullying](http://en.wikipedia.org/wiki/Cyberbullying) case involving the suicide of a girl harassed on [myspace](http://en.wikipedia.org/wiki/Myspace). Charges were under 18 USC 1030(a)(2)(c) and (b)(2)(c). Judge Wu decided that using [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 1030(a)(2)(C)](http://www.law.cornell.edu/uscode/18/1030.html#a_2_C) against someone violating a [terms of service](http://en.wikipedia.org/wiki/Terms_of_service) agreement would make the law overly broad. 259 F.R.D. 449
  + *People v. SCEA*, 2010. Class action lawsuit against Sony for removing [OtherOS](http://en.wikipedia.org/wiki/OtherOS), the ability to install and run Linux (or other operating systems) on the PlayStation 3. Consumers were given the option to either keep OtherOS support or not. SCEA was allegedly in violation of this Act because if the consumers updated or not, they would still lose system functionality.[[12]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-autogenerated6-12)
  + [*United States v. Drake*](http://en.wikipedia.org/wiki/Thomas_Andrews_Drake), 2010. Drake was part of a whistle-blowing effort inside the [NSA](http://en.wikipedia.org/wiki/NSA) to expose waste, fraud, and abuse with the [Trailblazer Project](http://en.wikipedia.org/wiki/Trailblazer_Project). He talked to a reporter about the project. He was originally charged with five [Espionage Act](http://en.wikipedia.org/wiki/Espionage_Act) counts for doing this. These charges were dropped just before his trial was to begin, and instead he pleaded guilty to one misdemeanor count of violating the CFAA, (a)(2), unauthorized access.
  + [*United States v. Bradley Manning*](http://en.wikipedia.org/wiki/United_States_v._Bradley_Manning), 2010-. [Bradley Manning](http://en.wikipedia.org/wiki/Bradley_Manning) was a soldier who allegedly disclosed tens of thousands of documents to those 'not entitled to receive' them. Among the 34 counts against him, there are several under (a)(1) and (a)(2) of the CFAA, some specifically linked to files like the [Reykjavik 13](http://en.wikipedia.org/wiki/Reykjavik_13) [State Department](http://en.wikipedia.org/wiki/State_Department) cable and a video of the [July 12, 2007 Baghdad airstrike](http://en.wikipedia.org/wiki/July_12,_2007_Baghdad_airstrike).[[13]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-13)
  + *Grand Jury investigation in Cambridge*, 2011. Unknown persons were listed in Grand Jury hearings in Cambridge, Massachusetts, regarding potential charges under the CFAA, as well as the [Espionage Act](http://en.wikipedia.org/wiki/Espionage_Act). Journalist [Glenn Greenwald](http://en.wikipedia.org/wiki/Glenn_Greenwald) has written these were likely related to [Wikileaks](http://en.wikipedia.org/wiki/Wikileaks).[[14]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-14)
  + [*United States v. Aaron Swartz*](http://en.wikipedia.org/wiki/United_States_v._Aaron_Swartz), 2011. [Aaron Swartz](http://en.wikipedia.org/wiki/Aaron_Swartz) allegedly entered an MIT wiring closet and set up a laptop to mass-download articles from[JSTOR](http://en.wikipedia.org/wiki/JSTOR). He allegedly avoided various attempts by JSTOR and MIT to stop this, such as [MAC address spoofing](http://en.wikipedia.org/wiki/MAC_address_spoofing). He was indicted for violating CFAA provisions (a)(2), (a)(4), (c)(2)(B)(iii), (a)(5)(B), and (c)(4)(A)(i)(I),(VI).[[15]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-15) The case was dismissed after Swartz committed [suicide](http://en.wikipedia.org/wiki/Suicide) in January 2013.[[16]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-16)
  + [*Sony Computer Entertainment America v. George Hotz*](http://en.wikipedia.org/wiki/Sony_Computer_Entertainment_America_v._George_Hotz) and Hotz v. SCEA, 2011. SCEA sued "Geohot" and others for [jailbreaking](http://en.wikipedia.org/wiki/Privilege_escalation) the PlayStation 3 system. The lawsuit alleged, among other things, that Hotz violated [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 1030(a)(2)(c)](http://www.law.cornell.edu/uscode/18/1030.html#a_2_c) ([by] taking info from any [protected computer](http://en.wikipedia.org/wiki/Protected_computer)). Hotz denied liability and contested the Court's exercise of personal jurisdiction over him.[[17]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-17) The parties settled out of court. The settlement caused Geohot to be unable to legally [hack](http://en.wikipedia.org/wiki/Hack_(computer_security)) the [PlayStation 3](http://en.wikipedia.org/wiki/PlayStation_3) system furthermore.
  + [*United States v. Nosal*](http://en.wikipedia.org/wiki/United_States_v._Nosal), 2011. Nosal and others allegedly accessed a [protected computer](http://en.wikipedia.org/wiki/Protected_computer) to take a database of contacts from his previous employer for use in his own business, violating 1030(a)(4)[[18]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-18)[[19]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-19) This is a complex case with two trips to the Ninth Circuit, and another seen as likely after the latest conviction in 2013.[[20]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-20)
  + [*Lee v. PMSI, Inc.*](http://en.wikipedia.org/wiki/Lee_v._PMSI,_Inc.), 2011. PMSI, Inc. sued former employee Lee for violating the CFAA by browsing Facebook and checking personal email in violation of the company's [acceptable use policy](http://en.wikipedia.org/wiki/Acceptable_use_policy). The court found that breaching an employer's acceptable use policy was not "unauthorized access" under the act and, therefore, did not violate the CFAA.
  + [*United States v. Peter Alfred-Adekeye*](http://en.wikipedia.org/wiki/Cisco_Systems#Antitrust_lawsuit) 2011. Adekeye allegedly violated (a)(2), when he allegedly downloaded [CISCO](http://en.wikipedia.org/wiki/CISCO) [IOS](http://en.wikipedia.org/wiki/Cisco_IOS), allegedly something that the CISCO employee who gave him an access password did not permit. Adekeye was CEO of [Multiven](http://en.wikipedia.org/wiki/Multiven) and had accused CISCO of [anti-competitive](http://en.wikipedia.org/wiki/Anti-competitive) practices.[[21]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-21)
  + *Pulte Homes v. Laborers' International Union of North America et al.* 2011. [Pulte Homes](http://en.wikipedia.org/wiki/Pulte_Homes) brought a CFAA suit against the [Laborers' International Union of North America](http://en.wikipedia.org/wiki/Laborers%27_International_Union_of_North_America) (LIUNA). After Pulte fired an employee represented by the [union](http://en.wikipedia.org/wiki/Labor_union), LIUNA urged members to [call](http://en.wikipedia.org/wiki/Telephone_call) and send [email](http://en.wikipedia.org/wiki/Email) to the company, expressing their opinions. As a result of the increased traffic, the company's [email system](http://en.wikipedia.org/wiki/Email_server) [crashed](http://en.wikipedia.org/wiki/Crash_(computing)).[[22]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-22)[[23]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-23)
  + *United States v*[*Sergey Aleynikov*](http://en.wikipedia.org/wiki/Sergey_Aleynikov), 2011. Aleynikov was a programmer at [Goldman Sachs](http://en.wikipedia.org/wiki/Goldman_Sachs) accused of copying code, like [high-frequency trading](http://en.wikipedia.org/wiki/High-frequency_trading)code, allegedly in violation of 1030(a)(2)(c) and 1030(c)(2)(B)i-iii and 2. This charge was later dropped, and he was instead charged with theft of[trade secrets](http://en.wikipedia.org/wiki/Trade_secret) and transporting stolen property.[[24]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-24)[[25]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-25)
  + [*United States v Nada Nadim Prouty*](http://en.wikipedia.org/wiki/Nada_Nadim_Prouty), circa 2010.[[26]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-26) Prouty was an FBI and CIA agent who was prosecuted for having a fraudulent marriage to get US residency. She claims she was persecuted by a U.S. attorney who was trying to gain media coverage by calling her a terrorist agent and get himself promoted to a federal judgeship.[[27]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-frogs1-27)
  + [*United States v. Neil Scott Kramer*](http://en.wikipedia.org/wiki/United_States_v._Neil_Scott_Kramer), 2011. Kramer was a court case where a cellphone was used to coerce a minor into engaging sex with an adult. Central to the case was whether a cellphone constituted a computer device. Ultimately, the United States Court of Appeals for the Eighth Circuit found that a cell phone can be considered a computer if "the phone perform[s] arithmetic, logical, and storage functions", paving the way for harsher consequences for criminals engaging with minors over cellphones.[[28]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-us_v_neil_scott_kramer-28)
  + [*United States v. Kane*](http://en.wikipedia.org/w/index.php?title=United_States_v._Kane&action=edit&redlink=1), 2011. Exploiting a [software bug](http://en.wikipedia.org/wiki/Software_bug) in a [poker machine](http://en.wikipedia.org/wiki/Poker_machine) does not constitute hacking[[29]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-29) because the poker machine in question was not a “protected computer” under the statute (not being connected to the [Internet](http://en.wikipedia.org/wiki/Internet) it was judged not to qualify as "protected computer" affecting[interstate commerce](http://en.wikipedia.org/wiki/Interstate_commerce)) and because the sequence of button presses that triggered the bug were considered "not exceed their authorized access." As of November 2013 the defendant still faces a regular [wire fraud](http://en.wikipedia.org/wiki/Wire_fraud) charge.[[30]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-30)
  + [*Craigslist v. 3Taps*](http://en.wikipedia.org/wiki/Craigslist_v._3Taps), 2012. 3Taps was accused by [Craigslist](http://en.wikipedia.org/wiki/Craigslist) of breaching CFAA by circumventing an [IP block](http://en.wikipedia.org/wiki/IP_address_blocking) in order to access Craigslist's website and [scrape](http://en.wikipedia.org/wiki/Web_scraping) its classified ads without consent. In August 2013, US federal judge found 3Taps's actions violated CFAA and that it faces civil damages for “unauthorized access”. Judge [Breyer](http://en.wikipedia.org/wiki/Charles_R._Breyer) wrote in his decision that "the average person does not use “[anonymous proxies](http://en.wikipedia.org/wiki/Anonymous_proxies)” to bypass an IP block set up to enforce a banning communicated via personally-addressed [cease-and-desist letter](http://en.wikipedia.org/wiki/Cease-and-desist_letter)".[[31]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-31)[[32]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-32) He also noted "Congress apparently knew how to restrict the reach of the CFAA to only certain kinds of information, and it appreciated the public v. nonpublic distinction — but [the relevant section] contains no such restrictions or modifiers."[[33]](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#cite_note-33)

Identity Theft

Identity Theft and Assumption Deterrence Act

* + [18 U.S.C. § 1028](http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00001028---A000-.html); [Wikipedia](http://en.wikipedia.org/wiki/Identity_theft) (*See* sectionentitled“United States”)
* (a) Whoever (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.
* + **In a Nutshell:** Makes the possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime, alongside unlawful possession of identification documents.
* + Permission is not lawful authority *Flores-Figueroa v. US, 551*
  + *Person:* Living or deceased *US v. Marcela-Abala*
  + Amended 18 U.S.C. § 1028 ("Fraud related to activity in connection w/ identification documents, authentication features, and information")
  + **Enforcement by Federal Authorities**
    - For federal jurisdiction to prosecute, the crime must include an "identification document" that either:
      * (a) is purportedly issued by the U.S.
      * (b) is used or intended to defraud the U.S.
      * (c) is sent through the mail, or
      * (d) is used in a manner that affects interstate or foreign commerce.  [**18 U.S.C. § 1028(c)**](http://www.law.cornell.edu/uscode/18/1028.html)
    - Grants FTC  authority to track # of incidents and $ value of losses, mainly re: consumer financial crimes (not all identification-based crimes)
    - **Punishment (Federal)**
      * Max 5, 15, 20, or 30 years in federal prison + fines, depending on the underlying crime [**18 U.S.C. § 1028(b)**](http://www.law.cornell.edu/uscode/18/1028.html)
      * Punishments for the unlawful use of a "means of identification" were strengthened in § 1028(a) ("Aggravated Identity Theft"), allowing for a consecutive sentence under the felony violations enumerated in § 1028A(c)(1) to (11).
  + **Enforcement by State or Local Law Enforcement Agencies**
    - **Penalties:** Different penalties apply depending on the state

Notification of Identity Theft

* Most states have enacted mandatory data breach notification laws, following CA’s lead
* As a result, companies that report a data breach typically report it to all their customers.[[56]](http://en.wikipedia.org/wiki/Identity_theft#cite_note-56)

Spam

CAN-SPAM Act of 2003

* + **15 U.S.C. § 7701-7706;** [**Wikipedia**](http://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003)
  + Establishes the first national standards for the sending of commercial e-mail
  + Requires the FTC to enforce its provisions

Spam

* **Spamming** – The process of sending out thousands to millions of unsolicited messages advertising products, spreading malware, or an attempt to phish people’s personal info
* A false or misleading statement is considered material if the alteration or concealment of header info would impair the ability of an IAS provider or a recipient to identify locate, or respond to a person who initiated the e-mail. *Facebook v. Power Ventures, 558*
* (b) Congressional determination of public policy (*based on the findings in (a)*) **15 U.S.C. § 7701(b)**
  + (1) there’s a substantial gov’t interest in regulating commercial e-mail on a nationwide basis;
  + (2) senders [shouldn’t] mislead recipients as to the source or content […]; **&**
  + **(3)** recipients […] have a right to decline to receive add’l commercial e- mail from the same source.
* **15 U.S.C. § 7704-7706**
* **Exceeds Authorized Access*****See* CFAA, 18 U.S.C. § 1030(e)(6)**
  + To access a computer w/ authorization and to use such access to obtain or alter info in the computer that the accesser is not entitled so to obtain or alter
  + *US v. Nosal, 572*
    - “Exceeds Authorized Access” in the CFAA doesn’t extend to violations of use restrictions
    - e.g., limited to violations of restrictions on access to info (not restrictions on its use)
    - Ct takes a narrower approach b/c it prohibits criminalization of minor user-agreement violations
    - The circuits are still divided. *See* broad approach in *US v. John F3d 263 (5th):*

*The question before us is whether “authorized access” or “authorization” may encompass limits placed on the use of information obtained by permitted access to a computer system and data available on that system. We conclude that it may, at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.*

Phishing and Botnets

* **Fraud & Related Activity in Connection w/ e-mail 15 U.S.C. § 1037**
* **Phishing**
  + Fraudulently soliciting consumers for personally identifiable info
  + Generally, a **botnet** sends 1000s of emails
* *FTC v. Pricewert LLC* 
  + An internet service provider (ISP) that participated in the distribution of spam, child porn, & other harmful e-content was permanently restrained and enjoined from recruiting or willingly distributing or hosting such content. Specifically, the provider could no longer recruit or willingly distribute or host child porn, botnet command and control servers, spyware, viruses, trojan horses, phishing-related sites, or similar electronic code or content that inflicted harm upon consumers. The provider failed to answer the FTC’s complaint under the **Federal Trade Commission Act**. DCt entered a default and a permanent injunction against the ISP. Federal Trade Commission Act, §§ 5(a), 13(b), [15 U.S.C.A. §§ 45(a)](https://a.next.westlaw.com/Link/Document/FullText?findType=L&pubNum=1000546&cite=15USCAS45&originationContext=document&transitionType=DocumentItem&contextData=(sc.UserEnteredCitation)#co_pp_8b3b0000958a4), [53(b)](https://a.next.westlaw.com/Link/Document/FullText?findType=L&pubNum=1000546&cite=15USCAS53&originationContext=document&transitionType=DocumentItem&contextData=(sc.UserEnteredCitation)#co_pp_a83b000018c76).

Music and Software Piracy

Criminal Policy

No Electronic Theft Act

* **Purpose:** To combat music and software piracy
* **Includes:** 17 U.S.C.A. §506 Criminal Offenses
  + **(a) Criminal infringement**
    - **(1) In general.**--Any person who willfully infringes a copyright shall be punished as provided under 18 U.S.C. § 2319, if the infringement was committed--
      * (A) for commercial advantage or private financial gain **or**
      * (B) by reproducing or distributng, including by electronic means, during any 180-day period, of 1+ copies or phonorecords of 1+ copyrighted works, which have a total retail value of < $1,000; **or**
      * **(C)** by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to the public, if such person knew or should have known the work was intended for commercial distribution.
    - **(2) Evidence** of reproduction or distribution of a copyrighted work, by itself, is insufficient to establish willful infringement of a copyright.

Theft of Proprietary Economic Info and Trade Secrets

Economic Espionage Act of 1996 (EEA)

* + **Purpose:** To combat theft of proprietary economic info
  + **Includes: Theft of Trade Secrets 18 U.S.C. § 1832(a)&(b)**
  + *US v. Aleynikov, 566*
    - Relies on *Dowling* for the proposition that the theft & subsequent interstate transmission of purely intangible property is beyond the scope of the NSPA
    - His system was neither “produced for” nor “placed in” interstate or foreign commerce b/c Goldman & Sachs had no intent to sell it
    - Congress later enacted legislation to close this loophole in the EEA. It now includes protection for *“any product or service used in or intended for use in” interstate commerce*

Evidence

Internet Evidence

*US v. Bynum, 575*

* **Analog**: Continuous wave
* **Digital**:Discrete

Search & Seizure

* *US v. Comprehensive Drug Testing, Inc, 579*
  + Extends *Tamura* to apply to e-searches
  + Basically, the issue is where they’re going to draw the line on what’s permittable when e-records are seized
  + *Tamura*
    - Applies to over-retrieval of info authorized under a search warrant

# PRIVACY

(Missed Class 9/9 Absence #1)

Government Collection and Disclosure of Personal Information

Controlled Substances

* + Patient-ID req’ts in NY State Controlled Substances Act of 1972 on the reputation or independence of patients on Sch. II controlled substances *Whalen v. Roe*

Interception of Communications

* **US PATRIOT Act Pub L. 107-056 (2001)**
  + Gives Federal officials greater authority to track and intercept communications for law enforcement and foreign intelligence purposes

Restricting Use by the Gov’t of Information in Gov’t Records

Counterintelligence Access to Telephone Toll and Transactional Records

**18 USC § 2709 (a-f)**

Stored Communications Act (SCA)

***42 USC 1983; 18 USC 2701***

*City of Ontario, CA v. Quon*

* + Ct took narrow approach and just looked at
    - whether he had a REP in his text messages sent on the pager provided to him by his employer
    - *Whether there was a search w/in the meaning of the 4th Amendment*
    - *and whether his EM’s search was reasonable under the circs*

ISP has no CL duty to police websites *Doe v. GTE Corp, 658*

*In re Google Inc Street View Electronic Communications Litigation*

* + **Readily accessible to the general public**" means, w/ respect to a radio communication, that such communication is not--
    - (A) scrambled or encrypted;

Private Collection and Disclosure of Information

Federal Wiretap Act

* **18 USC § 2511**
  + It has evolved over time. Originally it was phone communications. Then they revised it to radio communication (no wire) and there’s a question of whether it applies to WiFi
  + *In re Google Inc. Street View Electronic Communications Litigation*
  + *Reno v. Condon* 528 U.S. 141

Electronic Communications & Privacy Act (ECPA)

* + (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--
    - (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the
    - general public;
    - (ii) to intercept any radio communication which is transmitted--
      * (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
      * (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
      * (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
      * (IV) by any marine or aeronautical communications system;
    - (iii) to engage in any conduct which--
      * (I) is prohibited by section 633 of the Communications Act of 1934; or
      * (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;
  + (iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
  + (v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

Children’s Online Privacy Protection Act (COPPA)

* 15 USC 6501
* *In re Google Inc. (Google Buzz)*

Privacy of Internet Users

Digital Millennium Copyright Act

* **17 USC 512(h)**
* Recording Industry Assoc. of America, Inc. v. Verizon Internet Services, 688

# Right to Accuracy of Information, 713-735

pp. 713-735

## Databanks

*Beaudry, 713*

*Rivera v. County of Los Angeles*

* + Π Santiago Rivera filed suit against ∆s (County of LA; LA County Sheriffs Dept) after having been
  + He alleged a COA under 14 USC 1983 for violations of his 1st and 14th amendment rights.
  + § 1983 allows a person to sue state & local (not federal) officials who have violated your rights (*Bivers action)*
    - π must establish

1. deprived of constitutional rights by ∆ and EEs acting under color of state law
2. ∆s have customs or policies that amount to deliberate indifference
   1. Ct. said π failed to show that it was a reoccurring custom, so failed this prong of the test
3. That these policies are the moving force behind the constitutional violation
   * Claims 14th Amendment right to DP was violated b/c ∆ failed to use the info available to them to investigate whether he was the right person
     + Uses the *Matthews* balancing test to determine whether DP rights violated
       - Balance risk of \_\_\_\_ with government interest
         * He has an interest in not being incarcerated
         * Gov’t has an interest in
   * Ct is deciding on ∆’s MSJ

# REGULATion of INTERNET CONTENT, 737-781

* **2 Main Constitutional Issues**
  + Jurisdiction
  + First Amendment

Social Media – Defamation & Disparagement

* *DiFolco v. MSNBC Cable LLC 622 F.3d 104*
  + Defamation is a valid COA for posts on internet websites and forums when the wrongdoer states an opinion on false facts w/ knowledge of the falsity or probable falsity
* *CostCo Wholesale Corp and United Food and Commercial Workers Union, Local* p. 371
  + Ct found that ∆ violated §8(a)(1) of the Nat’l Labor Relations Acts by maintaining a rule prohibiting EE’s from electronically posting statements that damage the company or any persons reputation

Internet Discriminatory Advertising

* *Chicago Lawyers Committee for Civil Rights Under law, v. Craigslist, 744*
  + **Fair Housing Act** **§ 804(a)** forbids discrimination on account of race, religion, sex, or family status when selling or renting housing **42 USC 3604(a)**
  + Can’t sue the messenger just b/c the message reveals a 3P plan to engage in unlawful discrimination

Pornography and Indecency

Public Libraries

* *US v. American Library Assoc. 529 U.S. 194; p.*
  + **Children’s Internet Protection Act**
    - * A public library may not receive federal assistance to provide internet access *unless* it installs software to block images that constitute obscenity or child pornography, and to prevent minors from obtaining access to material that is harmful to them
  + **Holding:** Public libraries use of internet filtering software doesn’t violate their patrons 1A rights 🡪 CIPA doesn’t induce libraries to violate the constitution **&** is a valid exercise of Congress’s spending power.
  + **CIPA doesn’t impose an unconstitutional condition on public libraries**
  + The internet really isn’t a “designated public forum” b/c it requires the gov’t to make an affirmative choice to open up its property for use as a public forum
    - e.g. it’s intentional…

Intellectual Property Rights vs. Free Speech

Domain Names

* *CPC International v. Skippy, 756*
* **Whether a Domain Name receives First Amendment Protection** 
  + Commercial website 🡪 Ct has more leverage to overcome First Amendment grounds
  + Non-commercial website 🡪 Ct less likely to enjoin it to shut down

Anonymous and Pseudonymous communications

* *First Time Videos, LLC v. Does 1-500 276 F.R.D. 241*; p.760

Encryption Software and the First Amendment

* **2-Key Encryption**
  + **Private Keys:**
  + **Public Keys:** Anyone can use it to encrypt a message
* *Junger v. Daley* p.766
* *321 Studios v. Metro Golden Mayer Studios, 771*

Cyberbullying

* **Cyberbullylng:** When teens use the internet, cell phones, or other devices to send or post text or images intended to hurt or embarrass another person
* In *D.C. v. R.R*., the Court of Appeal for the Second District in California ruled that the message relayed in a case of cyberbullying must be unprotected by the First Amendment of the Constitution of the United States. For a statute to withstand constitutional scrutiny it must concern a substantial government interest and be narrowly tailored to achieve that interest using the least restrictive means necessary to achieve that interest.

Anti- Strategic lawsuit against public participation (Anti-SLAPP)

* *D.C. v. R.R. 182 Cal. App. 4th 1190 ;* p.776
  + Strategic lawsuit against public participation (SLAPP) Code Civ. Proc. § 425.16
  + CA Anti-SLAPP statute allows you to exercise a First Amendment Right
    - **TX** also has an anti-SLAPP statute
  + **First Amendment**
    - Ct uses objective standard of true threats: “statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals”
    - Need not intend to carry out the threat
    - A serious threat, not uttered in just idle talk, or political argument
    - Ct looks at subjective test: Would a reasonable person

# ELECTRONIC TRANSACTIONS (481-512)

Old and New Situations

Paper Transactions

* *Byers v. Intuit* ; p.482

Authentication of Signatures

Electronic Signatures in Global and National Commerce Act (The ESIGN Act)

**15 U.S.C. § 7001 (2006);** [**Wikipedia**](http://en.wikipedia.org/wiki/Electronic_Signatures_in_Global_and_National_Commerce_Act)

* **Purpose**
  + US federal law passed by the U.S. Congress to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.
  + Although every state has at least one law pertaining to e-signatures, federal law provides the guidelines for interstate commerce.
  + The general intent of the ESIGN Act is spelled out in § 101(a),
* **Signatures, generally § 101(a)**
  + A contract or signature “may not be denied legal effect, validity, or enforceability solely because it is in electronic form”. In sum, e-signatures and records are just as good as their paper equivalents, and therefore subject to the same legal scrutiny of [authenticity](http://en.wikipedia.org/wiki/Authentication) that applies to paper documents.[[3]](http://en.wikipedia.org/wiki/Electronic_Signatures_in_Global_and_National_Commerce_Act#cite_note-ps3-3)
  + A contract or other effect related to [an electronic] transaction
  + A valid signature may not be denied legal effect
* (2) **Electronic**: means form; and
  + (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.
* **Electronic signature**
  + A signature that is an electronic symbol or process, that is attached to or logically associated w/ a contract and
  + executed or adopted by a person with the intent to sign the record.
  + *Similar definition in the Uniform Electronic Transactions Act (see below)*
* **Right to Not Use E-Signatures § 101(b)**
  + Preserves the rights of individuals to not use electronic signatures
  + Individuals reserve the right to use a paper signature.
  + § 101 (c) directly supports (b) by requiring a “Consumer Disclosure”
    - *Consumer Disclosure*: The signatory has consented to use an electronic format
* **Must Reasonably Demonstrate the Subject of the Consent § 101(c)**
  + A consumer "consents electronically, in a manner that reasonably demonstrates that the consumer can access info in the electronic form that will be used to provide the info that is the subject of the consent"
* **Retention of Contracts and Records § 101(d)** 
  + If a law requires that a business retain a record of a transaction, the business satisfies the req’t by retaining an electronic record, as long as the record "accurately reflects" the substance of the contract **&**
  + is "accessible" to people who are entitled to access it "in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing or otherwise."

Uniform Electronic Transactions Act (UETA)

**7A, Part I, ULA 17 (Supp. 2000);** [**Wikipedia**](http://en.wikipedia.org/wiki/Uniform_Electronic_Transactions_Act)

* **Scope**
  + One of several US Uniform Acts proposed by the [National Conference of Commissioners on Uniform State Laws](http://en.wikipedia.org/wiki/National_Conference_of_Commissioners_on_Uniform_State_Laws) (NCCUSL)
  + 47 states, D.C., Puerto Rico and the Virgin Islands have adopted the UETA
* **Purpose:** To harmonize state laws re: retention of paper records (especially checks) and the validity of e-signatures
  + Authorizes the use of electronic documents and electronic-signatures instead of paper documents and paper signatures
  + Authorizes e-signatures and electronic records in place of paper record
  + Contains a very limited number of exceptions overrides
  + Following the inception of the Act, Congress adopted the Electronic Signatures in Global and National Commerce Act.
  + EX: of paper-free transactions: Mobile phone payments, tax filing
* **Electronic record**: A record created, generated, sent, communicated, received, or stored by electronic means **U.S.C. § 2(a)(7)**
* **Electronic signature** : An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
  + The e-signature must be linked or logically associated w/ the record
    - In paper transactions 🡪 it’s assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be authenticated
    - In electronic transactions 🡪 the symbol must in some way be linked to, or connected with, the electronic record being signed.
* **Scope U.S.C. § (3)**
  + Only applies to transactions related to business, commercial (including consumer) and governmental matters.
  + Unilaterally generated electronic records and signatures which are not part of a transaction also are not covered by this Act.
* **Applies:** to any e-record or e-signature created, generated, sent, communicated, received, or stored **U.S.C. § (4)**
* **Not req’d to be in electronic form and 5(b) states U.S.C. § (5)**
* (b) This [Act] applies only to transactions b/w parties each of which has agreed to conduct transactions by e-means. Whether the parties agree to conduct a transaction by e-means is determined from the context and circs, including the parties' conduct.

**Application and Purpose of the Act U.S.C. § 6**

To facilitate and promote commerce and govt’l transactions by validating and authorizing the use of e-records and e-signatures

**Legal recognition to e-signatures, records and contracts § 7**

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

**Information must be available to all parties § 8**

(a) ...An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(c) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

**Effect of e-record and e-signatures § 9**

(a) An e-record or e-signature is attributable to a person if it was the act of the person. May be shown in any manner, including a sh*owing of the efficacy of any security procedure applied to determine the person to which the e-record or e-signature was attributable.*

(b) The effect of an e-record or e-signature attributed to a person under (a) is determined from the context and surrounding circs at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.

**Change or errors in an e-record occurring in transmission § 10**

**A notary public and other authorized officers may act electronically, effectively removing the stamp/seal req’ts § 11**

**Retention of Records satisfied by retaining an e-record § 12**

*(a) If a law requires that a record be retained, the req’t is satisfied by retaining an e-record of the info in the record which:*

*(1) accurately reflects the info set forth in the record after it was first generated in its final form* ***&***

*(2) remains accessible for later reference.*

(b)

(c) A person may satisfy (a) by using the services of another person if the req’ts of (a) are satisfied.

**Evidence**

In a proceeding, evidence of a record or signature may not be excluded solely b/c it’s in electronic form**§ 13**

**Automated Transactions § 14**

*(1) discussed situations where "...contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements."*

*(2) applies to a contract that "may be formed by the interaction of an electronic agent and an individual".*

**"Time and Place" aspects of e-transmissions § 15**

* + **Comment 1.** This section provides default rules regarding when and from where an electronic record is sent and when and where an electronic record is received. This section does not address the efficacy of the record that is sent or received. That is, whether a record is unintelligible or unusable by a recipient is a separate issue from whether that record was sent or received. The effectiveness of an illegible record, whether it binds any party, are questions left to other law.

**Transferable records § 16**

* (c) A system satisfies (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:
  + (1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in (4), (5), and (6), unalterable;

**Optional Provisions States may adopt §§ 17-19**

* + Among the barriers to e-commerce are barriers which exist in the use of e-media by State governmental agencies - whether among themselves or in external dealing with the private sector.

Computer Fraud and Abuse Act

* *See* **Computer Fraud and Abuse Act 18 U.S.C. §1030;** Wikipedia
* *WEC Carolina Energy Solutions LLC, v. Miller 687 F.3d 199* ; p.488

Bankruptcy-Protecting Software Users

* **Bankruptcy Code 11 U.S.C. § 365**

Consumer Protection by the FTC

* *Federal Trade Comm. V. Accusearch Inc. p.494*

Communications Decency Act

* + **CDA on Westlaw; 47 U.S.C.A. § 230**
  + Shields the ISP a.l.a. they meet certain req’ts

* + **(c)(1) Protection for “Good Samaritan” blocking and screening of offensive material**
    - (1) Treatment of publisher or speaker
      * + No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

Taxations

* *Direct Marketing Assoc. V. Huber,*  ; p.497
  + **Holding:** The Act & regulations directly regulate and discriminate against out-of-state retailers. Therefore, interstate commerce…
  + **Rule, per prof:** Commerce Clause always trumps; state can’t favor its own law over the CC

Restricting E-Competition

* Certain types of businesses have obtained state legislation or court decisions limiting internet-based competition
* *Granholm v. Heald*  544 U.S. 460; p. 499
  + **Holding:** The laws in both States discriminate against interstate commerce in violation of the Commerce Clause Art. I § 8. The discrimination is unauthorized & not permitted by the 21st Amendment. Therefore, the laws were unconstitutional b/c they didn’t use the least restrictive means to accomplish the goal of preventing minors from obtaining alcohol from online retailors

Unlawful Internet Gambling Enforcement Act

* ***Interactive Media Entertainment and Gaming Assoc. v. Attorney General \_\_\_\_\_\_\_\_\_; p. 504***
  + A indivduals interest in gambling doesn’t rise to the level of sexual privacy in the home (*Lawrence)* .
  + Gambling is not a protected individual interest under any constitutionally protected right to privacy
  + **Holding:** The Act is constitutional
  + A state may enact legislation limiting or prohibiting or regulating gambling across state borders. May also enforce […]

US – Measure Affecting the Cross-Border Supply of Gambling and Betting Services

* *US v. Birbragherm*  603 F.3d 478 ; p. 509
  + RE: consipiracy to distribute controlled substances under the Controlled Substances Act (CSA)

# TELECOMMUNICATIONS and the Internet

*Pages 513-542*

Telecommunications Act of 1996

* + Encouraged competition among service providers
  + Allowed them to compete if they met criteria that demonstrated competition in that local market
  + Intent was to enhance competition, lower prices
* *Talk America, Inc. v. Michigan Bell Tel. Co.* ; p.
* *Quest Corp v. Minn. Public Utilities Comm.* ; p.520

Regulation of Internet Service Providers

* *National Cable & Telecommunications Assoc. v. Brand X Internet Services ; p.*524

IP-Enabled Communications

* *Minn. Public Utilities Comm. V. Federal Comm. Comm.* ; p.529
* *Vonage Holdings Corp. v. Nebraska Public Service Comm.* ; p.531

Carrier Traffic Management & Network Neutrality

* The debate is over the extent to which federal regulators may require ISP’s to carry traffic equally, w/o regard to content or source
* *Comcast Corp. v. Federal Communications Comm.* 600 F3d 642; p.536
  + ISPs have wide latitude in regulating their networks

Cloud Services

* **3 Models of Cloud Computing**
  + **Software as a Serve (SaaS)**: Provides the ability to use a 3P provider’s applications that are accessible to the user through an interface (such as a web browser)
  + **PaaS**: Provides an environment that allows the consumer to deploy and run their own independently developed applications
  + **IaaS**: Enables a consumer to deploy its own software including OS’ and applications, on networking and computing resources providers by a 3P provider

# TRADEMARK

*Pages 399-464*

Discipline

* *Rescuecom Corp v. Google p. 399*
* *Lens.com v. 1-800-Contacts p. 405*
* *Perfumebay.com, Inc v. eBay, Inc. p.412*

Lanham Act

* **Lanham Act**
  + To establish trademark infringement, a π must prove
    - Owns a valid mark
    - ∆ used the mark in commerce and 1/o π’s authorization
    - ∆ used the mark (or an imitation of it) in connection w/ the sale, offering for sale, distribution, or advertising of oods or services; **&**
    - ∆’s use of the mark is likely to confuse consumers
* **General**
  + Enforcement of trademark is intended to protect consumers, not necessarily about creative incentives.
  + Possible for a strong mark to eventually become generic and lose protection e.g., xerox, kleenex, blackberry, etc.
* **Requirements**
  + Use in a way to establish the connection with the mark and source of the goods or services
  + Use in commerce
  + They vary in strength from arbitrary/fanciful, suggestive, descriptive and generic.
* **Benefits of trademark**
  + Others can use it as long as it isn’t likely to cause confusion
  + Protection from dilution (use of the mark in a non-confusing way that takes away the marks esteem)
  + Protects from cybersquatting (domain name extortion)
    - “The registering of a domain name on the internet in the hope of selling or licensing it at a profit”
  + Can last forever
  + 2 companies with same name 🡪 whoever claims domain name 1st
* **Req’ts for there to be a trademark issue:** It’s only when there’s bad faith & intent to profit that there’s an issue

Confusion

* **3 Types of Confusion**
  + **Direct**: Likely to cause some consumers to believe that the π is the source of ∆’s G/S
  + **Reverse**: Who cares
  + **Initial interest/source**: Consumer seeks G/S of a certain TM holder and is lured to a competitor’s product b/c competitor used a similar mark.
* **Factors for finding confusion**
  + Similarity of the marks
  + Intent of the infringer in adopting the mark
  + Evidence of actual confusion
  + Similarity of product or manner of marketing
  + Strength or weakness of the marks
  + Competitive proximity of the G/S, quality of ∆’s products, sophistication of the buyers
* [*Virtual Works, Inc. v. Volkswagen of America, Inc.*](https://a.next.westlaw.com/Document/Ib6987e56799711d9bf29e2067ad74e5b/View/FullText.html?originationContext=docHeader&contextData=(sc.UserEnteredCitation)&transitionType=Document&docSource=cd9620b4f6a44041b7e97901f3bf9374) but see 5th cir. Maxwell house

Federal Trademark Dilution Act

* **Federal Trademark Dilution Act (FTDA) 15 USC § 1125(c)**
  + Amended Lanham Act
  + Provides a COA for dilution of a famous mark
  + Amended to allow an owner of a famous trademark to assert a claim based on a likelihood of dilution.
  + In response to ruling in *Mosely v. Secret Catalogue, Inc.,* which req’d πs to present evidence of actual dilution.
* *Rosetta Stone LTD v. Google, Inc. 676 F.3d 144; p.418*

Anti-Cybersquatting Consumer Protection Act

* **Purpose:** Cyberpiracy prevention
* **Relief Provided:** Allows for an owner of a trademark to bring an action against another (a.k.a., cybersquatter) who registers, traffics in, or uses a domain name in bad faith
* [**Anti-Cybersquatting Consumer Protection Act**](https://a.next.westlaw.com/Document/I7A99A490CFC511DEA64BC13F4D131DCF/View/FullText.html?listSource=Search&navigationPath=Search%2fv3%2fsearch%2fresults%2fnavigation%2fi0ad60406000001495861fe9e660ed8dd%3fNav%3dSTATUTE%26fragmentIdentifier%3dI7A99A490CFC511DEA64BC13F4D131DCF%26startIndex%3d1%26contextData%3d%2528sc.Search%2529%26transitionType%3dSearchItem&list=STATUTE&rank=3&listPageSource=8e04318218bb82c1dbde44e748cad327&originationContext=docHeader&contextData=(sc.Search)&transitionType=Document&docSource=81ea8730646c42c2b5827fc2c540a710) **14 USC § 1125(d)**
  + A person shall be liable in civil action by the owner of the mark, including a personal name which is protected if, w/o regard to the G/S of the parties, that person:
    - Has a bad faith intent to profit from that mark, including a personal name which is protected as a mark **&**
    - Registers, traffics in, or uses a domain name that:
      * + Is identical or confusingly similar
        + To a famous mark that’s famous at the time of registration **or**
        + Is a trademark, word, or name that’s protected
* **Requirements** *DSTP Int’l, Inc. v.Nahum; 624 F3d 1213, 1218-19 (9th Cir. 2010)*
  + 1) ∆ registered, trafficked in, or used a domain name **&**
  + 2) Domain name is identical or confusingly similar to a protected mark owned by π **&**
  + 3) ∆ acted w/ bad faith intent to profit from that mark
* **9 Factors of CYBERSQUATTING**
  + Interest of ∆, if any, in the mark
  + Extent that the domain name consists of a legal name of ∆
  + Prior use of the mark by ∆ in connection w/ a legit G/S
  + Bona fide non-commercial or fair use
  + Intent to divert customers
  + ∆’s offer to transfer or sell the mark w/o using it
  + Provision of false material when registering the domain
  + ∆’s use or ownership of multiple fake domain names.
  + Extent that the mark is distinctive or famous
* *Rearden LLC v. Rearden Commerce, Inc 683 F.3d 1190; p. 429*
  + Ct adopts req’ts listed above
* **Cyberpiracy protections for individuals 15 U.S.C.A. § 8131**
  + Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.
  + ***Unless*** in good faith

Domain Name Dispute Resolution

Uniform Domain Name Dispute Resolution Policy (UDRP) *(primary)*

* **General**
  + Est. by iCANN per US gov’ts request
  + Established through Dispute Resolution Service Providers e.g., WIPO
* **Applies to:** All generic top-level domains e.g..com, .org, .edu, .net, .biz, .info, etc.
* **Requirements to Register a Domain Name**
  + To register a domain name, registrant must represent and warranty that it won’t infringe or violate rights of any 3P and   
    agree to UDRP procedures if a claim is asserted
* **Complainant must show**
  + Identical or confusingly similar mark
  + Registrant doesn’t have any rights or legitimate interests
  + Registered in bad faith
* **Disadvantages** 
  + Fair use defense isn’t always embraced (b/c dealing w/ int’l bodies)
  + Bulk registrations not viewed favorably (b/c shows bad faith intent)
  + No injunctive relief, DAS, etc

*Dreamworks Animation LLC v. Phivos Morides/Phoebus Morides WTO Arbitration and Mediation Center, 2012*

*Case No. D2012-0054. p.435*

Uniform Rapid Suspension (URS) *(new, not utilized yet)*

* *New alternative, not really utilized yet*
* *Basically the same elements*
* **Applies to:** New, generic top-level domains
* **Disadvantages**
  + Domain names not transferred. Instead they’re suspended
  + No mechanism to trn
  + Registration re-initiates every term
* *Petroliam National Berhad v. GoDaddy.com, Inc*
  + SCOTUS in 10/2014 held that domain name registrar can’t be held liable for bad faith redirects placed through their domain name fwd’ing service

Defenses

Nominative Fair Use

*Playboy Enterprises, Inc. v. Terri Welles, Inc. 279 F.3d 796; p.441*

**Test**

* + Product or service in question must be one not readily identifiable w/o use of the trademark **&**
  + Only so much of the marks or marks may be used as is reasonably necessary to identify the product or service **&**
  + User must do nothing that would, in conjunction w/ the mark, suggest sponsorship or endorsement by the trademark holder

Functional Use

**General**

* + Arises from functionality doctrine, which is based in CL
  + Prohibited assertion of trademark rights in the functional features of a product or its packaging.
  + To distinguish b/w trademark and patent law

*Sega Enterprises Ltd. V. Accolade, Inc. 977 F.2d 1510; p.448*

Unfair Business Practices – unsolicited email

*Asis Internet Services v. Consumerbargaingiveways, LLC; p. 456*

# COPYRIGHT (1-186)

* **Rights of a copyright** (this sounds wrong – see the first outline)
  + Control the use
  + Exclude the use
  + Right of reproduction
  + Right to (publicly) display
  + Right to amend
* **Trade Secrets**
  + Weak stepsister to patent law
  + Secrets that are used in business to gain an advantage over others are protectable to an extent as long as they’re kept secret
  + Coincidental development is not protected and reverse engineering is fine
  + They’re protected from improper seizure, ex-employee, theft, etc.
  + Last forever if protected
* **Limits of Special Importance to Educators**
  + First Sale Doctrine
  + ..
* **Debunking Myths**
  + It’s not necessary to affix a copyright notice to a work in order to preserve the copyright
  + Using any part of a copyrighted work is an infringement unless the use qualifies as of the copyright protections
  + Giving an author credit may avoid an academic charge of plagiarism, but it is not a defense to an infringement claim
  + Modifying an original work violates the author’s exclusive right to create derivative works
  + On the internet, the rules of copyright do not change simply b/c of a change of medium
* **3 Questions to Evaluate whether you can use it**
  + (1) Is the work protected?
    - * EXs of non-protected works
  + (2) IF the work is protected, do you wish to exercise one of the owner’s exclusive rights?
    - * Make a copy
      * ….
      * …
      * ..
  + (3) Is your use exempt or excused from liability for infringement

Fair Use

* **4 Factor Fair Use Test**
  + 1. What’s the character of the use?
    - * **🡨 Fair Use ------------- ---------🡪 Not fair use**
      * Nonprofit Criticism Commercial
      * Educational
      * Personal
      * Small amount Large amount
      * Non critical part key points

Original is out of print or otherwise unavailable

No ready market for permission

…

* + 2. What’s the nature of the work to be used
  + 3. How much of the work will be used?
  + 4. What would the effect of the use be upon the potential market for the original copyrighted work?
* **Defenses**
  + Good Faith Fair Use Defense

Liability & Torts

Trespass to Chattels

* **To win, π must show**
  + Chattel w/ ownership interest
  + **Trespass to chattels IF:**
    - * ∆ dispossess owner of the chattel
      * Chattel is impaired w/ regards to condition, quality or value
      * Possessor is deprived of use for a substantial period of time
      * Bodily harm to a person or something in which π has a legally protected interest

Intentional trespass

* + Harm suffered
* *CompuServe v. Cyberpromotions*
  + Electronic Signals are sufficiently physically tangible for a trespass claim
  + Value can be diminished by such signals
  + Provider was not a public utility, so D did not enjoy a special privilege to use
  + Company had adequate means of communication available to it

iCANN-SPAM – pre-empts state anti-spam laws

* **Marketers must comply with regulations re:**
  + **Unsubscribing**: Must provide a visible and operable unsubscribe mechanism and honor such requests w/in10 days
  + **Content**: Accurate “from” lines, relevant and non-deceptive subject line, disclaimers for adult material
  + **Sending behavior**: Message can’t be sent to “harvested” e-mail addresses and can’t contain false headers
* **For a private right of action under CAN-SPAM, π must show:**
  + ∆ either sent e-mail in violation of the above or paid someone else to do it know sender would act in violation
  + Adverse effects that amount to more than time and money involved in dealing with spam
* **Exemptions include:**
  + Religious or political message
  + Content that complies broadly with marketing mechanism specified in law **&**
  + National security messages.

Defamation

* **CDA**
  + No provider or user of an interactive service shall be treated as a publisher or speaker of any information provided by another information content provider
  + No provider or user is liable for
    - * Any action voluntarily taken in good faith to restrict access to or availability of material the provider considers to be obscene, lewd, etc., regardless of whether the material is constitutionally protected
      * Any action taken to enable or make available to information content providers or other means to restrict access to such material.

Misappropriation

* + ∆ appropriated π’s name or likeness for the value associated with it, without consent, P can be identified from the publication, and or benefit to the ∆.

Electronic Communications Privacy Act of 1986 (ECPA)

* **Electronic Communications Privacy Act of 1986 (ECPA)** [Wikipedia](http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act)
  + **Title I 18 U.S.C. § 2510**
    - Protects wire, oral, and electronic communications while in transit
    - Provides more stringent search warrant req’ts
    - It’s an offense to intentionally intercept, endeavor to intercept or to procure any other person to intercept any wire, oral or electronic communication
    - Each e-mail, while traveling through wires, is an electronic communication and doesn’t cease being so during momentary intervals intrinsic to the communication process, at which the message resides temporarily in transient storage.
  + **Title II: The Stored Communications Act 18 U.S.C. § 2101**
    - Protects communications held in electronic storage, most notably, messages stored on computers.
    - Protections are weaker than Title I. No heightened standards for warrants.
    - Stored commendations. Has a lower penalty.
  + **Title III** **18 U.S.C. § 3121**
    - Prohibits the use of pen register and/or trap and trace devices to record dialing, routing, addressing, and signaling info used in the process of transmitting wire or electronic communications w/o a court order.
* **Electronic Communications:** Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photoelectronic or photooptical system that affects interstate or foreign commerce
  + **Excludes**
    - Wire or oral communication
    - Communication made through a tone-only pager
    - Communication from a tracking device (defined in § 3117)
    - Electronic funds transfer info stored by a financial institution in a communications system used for the electronic storage and transfer of funds
* **Remedy:** ECPA doesn’t give suppression as a remedy, only civil and criminal punishments.

Computer Fraud and Abuse Act (CFAA)

* **Computer Fraud and Abuse Act 18 U.S.C. §1030;** [Wikipedia](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act)
* **Protected Computers**  **18 U.S.C. § 1030(e)(2)** 
  + Exclusively for the use of a financial institution or the US gov't, or,   
    if not exclusively for such use, used by or for a financial institution or the US gov't and the conduct constituting the offense affects that use by or for the financial institution or the gov't **or**
  + Used in or affecting interstate or foreign commerce or communication, including a computer located outside the US that’s used in a manner that affects interstate or foreign commerce or communication of the US
* **Criminal offenses under the act** 
  + Knowingly accessing a computer w/o authorization in order to obtain national security data
  + Intentionally accessing a computer w/o authorization to obtain:
    - * Info contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.
      * Info from any department or agency of the United States
      * Info from any protected computer if the conduct involves an interstate or foreign communication
  + Intentionally accessing without authorization a gov't computer and affecting the use of the gov'ts operation of the computer.
  + Knowingly accessing a protected computer with the intent to defraud and there by obtaining anything of value.
  + Knowingly causing the transmission of a program, information, code, or command that causes damage or  
    intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in:
    - * Loss to 1+ persons during any one-year period aggregating at least $5,000 i
      * The modification or impairment, or potential modification or impairment, of the medical exam, diagnosis, treatment, or care of 1+ individuals.
      * Physical injury to any person.
      * A threat to public health or safety.
      * Damage affecting a gov't computer system
  + Knowingly and with the intent to defraud, trafficking in a password or similar info through which a computer may be accessed w/o authorization.

He wrote basic bookkeeping and accounting for lawyers

Texas Identity Theft Enforcement and Protection Act

**Texas Identity Theft Enforcement and Protection Act Tex. Bus. And Com. Code § 521.001**

* + Business Duty to protect sensitive info **Tex. Bus. And Com. Code § 521.052**
  + Add’l penalties of up to $20,000 (per violation?) if you provide reasonable assurance to customers of the confidentiality of their information and then fail to provide it.