Info Privacy Outline

I. INTRODUCTION

***A. Information Privacy Law: Origins and Types***

I. Common Law

1. Developments in the late 19th century created a growing interest in privacy
   1. Press became increasingly sensationalistic; yellow journalism
   2. Technological developments caused great alarm for privacy
2. Warren and Brandeis: *The Right to Privacy*
   1. Privacy Right in CL: **Right to be let alone**
      1. Scope includes life, bodily injury, nuisance, emotional distress, literary property, defamation, k law, etc…
   2. Exception: Right to be let alone, **except for matters of general or public interest**
      1. Focuses on “obvious bounds of propriety and decency”
      2. Scope of the right is class and culturally based
      3. Ability to control what is being written and said about ourselves
   3. **Right of Inviolate Personality**: Literary Property & Defamation
      1. The right is held within the individual
         1. Not the property that matters, rather the intellectual content
         2. Goes beyond protecting ones reputation
      2. WB argue for liability for printing someone else’s literary content, even if not word-for-word
         1. Cites to *Prince Albert v. Strange*, where Albert draws pictures, but court said that they are protected from publishing under the crown (even descriptions of the pictures are forbidden)
   4. **Rights as Against the World**: Contract Law
      1. Implied k is a right as against the world
         1. Situation where court determines that the law needs to be extended, even though the written k may not have established that point
         2. Courts continued this process, not legislatures or statutes
      2. WB argue that courts need to continue the extension of rights, and protect privacy as rights against the world
         1. Typically envision rights against the world as established constitutions that provide unalienable rights
         2. Highlights crucial role that courts have in developing privacy rights
3. W&B: Limitations/Defenses to the Right to Privacy (drawn from libel and slander)
   1. Privacy does not prohibit any publication of matter which is of public or general interest
   2. Right to privacy does not prohibit communication when the publication is made under circumstances which would make it privileged under libel and slander
      1. If privileged in a defamation action, also privileged in a privacy action
      2. Essentially right does not carry over to common law privileges; reporting a crime or confessions to a priest
   3. Oral publications have a higher standard of proof
      1. Difficult to make a reasonable determination
      2. Injury is so trifling that it should be disregarded for sake of free speech (as in libel)
   4. Right to privacy ceases upon publication of the facts by the individual or with his consent
      1. Another defamation action rewritten for privacy
   5. Truth of the matter published does not provide a defense
      1. This is not another defamation action
      2. Privacy is more violative if the matter is true; but if matter is false than defamation is established
   6. The absence of malice in the publisher does not provide a defense
      1. Malice is a defamation concept, as it was required for punitive damages
4. W&B: Remedy for Invasion of the Right to Privacy
   1. Right to privacy is effectively a defamation action
      1. Action of tort for damages in all cases; even w/o special damages, substantial compensation could be allowed for injury to feelings (as in action for L/S)
      2. Injunctions in a limited class of cases
      3. No recovery for something of general/public interest
      4. No recovery if individual personally consents to making information public
   2. No criminal remedy
      1. Legislation would be required for privacy protection in the criminal scope
   3. Privacy action differs from Defamation action
      1. No 3rd party needed to establish harm cause; Victim acts as own witness
      2. No requirement of malice
      3. Truth is not a defense
5. Recognition of Warren and Brandeis Privacy Torts
   1. *Roberson v. Rochester Folding Box*: NY Court of Appeals refused to recognize common law tort action for privacy invasions; led to NY legislature creating a privacy tort action by statute in 1903
   2. *Pavesich v*. *NE Life Insurance*: Georgia became the first state to recognize a common law tort action for invasion of privacy in 1905
      1. Newspaper published an advertisement with a photo of plaintiff w/o consent
6. Four Torts for Invasion of Privacy: William Prosser’s *Privacy*; R2d of Torts
   1. Intrusion upon seclusion
      1. Unreasonable intrusion
         1. Shocking or outrageous
         2. Not a matter of public interest
         3. Same exclusions as W&B apply
      2. Actual solitude or seclusion must be intruded upon
   2. Public disclosure of private facts
      1. Publicity must be of no legitimate concern to public
      2. Highly offensive to a reasonable person
   3. False light
      1. Publicity that unreasonably places someone in a false light before the public
      2. Resembles a defamation claim; recognized in bare majority
      3. Other torts are recognized in most states
   4. Appropriation
      1. Economic and property tort, rather than a privacy tort
         1. Only applies for advertising and endorsements; commercial context
      2. Remedy exists against one who appropriates to his own use or benefit the name or likeness of the plaintiff
         1. Intrusion into someone’s privacy by appropriating name, image, signature, or voice, etc…
7. Effectiveness of Prosser’s Torts for Invasion of Privacy
   1. SCOTUS has permitted but restricted these torts
      1. 1st amendment argument: Constitutional limit on these torts because of ability to impinge on free speech
   2. Very rare to win on one of these torts if suing a publisher, speaker, broadcaster
      1. Courts often view tortfeasor’s act as informing the public, triggering first amendment protection
      2. Often win invasion of privacy in a narrow circumstance
   3. Not widely used; difficult to win; Potentially very expensive
8. Additional Privacy Torts
   1. Breach of confidentiality: remedy when a professional divulges a patient or client’s confidential information
   2. Defamation: liability when one makes a false statement about a person that harms the person’s reputation (limited under 1st amendment)
   3. Infliction of emotional distress: remedy when one, by extreme and outrageous conduct, intentionally or recklessly causes severe emotional distress to another; as privacy invasion can often result in severe emotional distress
9. Other Sources of Privacy Protection
   1. Evidence Law
      1. Under CL, certain communications are privileged, and hence cannot be inquired into during legal proceedings: attorney and client, priest and penitent, husband and wife, physician/psychotherapist and patient
   2. Property Rights
      1. Trespass: ability to exclude others from the land and air you own
      2. Appropriation and Personal information torts implicate property
   3. Contract Law
      1. Action for breach of implied k or tort actions based on implicit duties once certain (fiduciary) relationships are established; e.g., AC privilege
      2. Focus on enforceable rights (non-disclosure agreement; employer agreement)
   4. Criminal Law
      1. W&B noted that situationally, criminal law would be appropriate to protect privacy
         1. Privacy of one’s home is protected by criminal sanctions for trespass
         2. Stalking and harassment can give rise to criminal culpability
      2. Many statutes protecting privacy also contain criminal penalty (e.g. identity theft)
   5. Constitutional Law
      1. Focus on criminal procedure rights, see below

II. Constitutional Law

1. Federal Constitutional Law
   1. US constitution does not specifically mention privacy
      1. Number of provisions do actually protect privacy and has been interpreted as providing a right to privacy
      2. No uninhibited right to privacy, but 4th amendment is the closest example
         1. Sets standard of reasonable expectation of privacy (*Katz*)
   2. 1st Amendment: In some instances safeguards privacy; e.g., right to speak anonymously
      1. Right of association means individuals can associate freely in private
      2. Membership organizations do not have to reveal member lists unless the state has a compelling interest
   3. 3rd Amendment: Protect privacy of the home by preventing government from requiring soldiers to reside in people’s homes
   4. 4th Amendment: People have the right to be secure in their persons, houses, papers and effects against unreasonable searches and seizures
      1. *Olmstead v. US*: wiretapping was not an invasion of privacy under 4th amendment bc it was not a physical trespass into the home
         1. *Brandeis’ dissent* argues for right to be let alone in both common law roots but under 4th amendment as well
      2. Modern 4th amendment analysis incorporates much of Brandeis’ view
         1. *Katz v. US*: 4th amendment protects people, not places
   5. 5th Amendment: Privilege against self-incrimination protects privacy by restricting ability of the government to force individuals to divulge certain information
   6. 14th Amendment: Individual constitutional right to privacy under DPC
      1. *Griswold v. Connecticut:* This right was located within the penumbras or zones of freedom created by expansive interpretation of the Bill of Rights
      2. *Whalen v. Roe*: extended its substantive due process privacy protection to information privacy, zone of privacy protected by the constitution encompasses the individual interest in avoiding disclosure of personal matters
   7. Number of states have directly provided for the protection of privacy in their own constitutions

III. Statutory Law

1. In the modern age (1970 – present), privacy protection emerges in statutory regulation
   1. Statutes take on a significant role, and the regulations interpreting those statutes have become the most important
   2. Throughout the 1970’s and 80’s, proliferation of privacy laws was in response to data mainframes emerging and the fear surrounding ability of computers to store and search for personal information
2. Code of Fair Information Practices
   1. Number of basic information privacy principles that allocate rights and responsibilities in the collection and use of personal information
3. Legislation has been passed to protect privacy in various sectors of the information economy, collection of sensitive personal data or facilitated government investigation techniques

***B. Perspectives on Privacy***

I. Perspectives and Critiques on Privacy

1. Alan Westin: *Privacy of Freedom*
   1. Focuses on (4) **elements of** **control**: Claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others
      1. **Solitude**: Individual separated from the group and freed form observation of other persons; most complete state of privacy for an individual
      2. **Intimacy**: Individual acts as part of a small unit that claims and is allowed to exercise seclusion so that it may achieve close, relaxed and frank relationship
      3. **Anonymity**: Individual is in public places or performing public acts, gut still seeks and finds freedom from identification and surveillance; anonymous publication
      4. **Reserve**: Creation of a psychological barrier against unwanted intrusion; limiting communication by the willing discretion of those around him; most subtle form
   2. The (4) **functions that privacy performs**:
      1. **Personal autonomy**: development of individuality and consciousness of individual choice in life; individual’s sense that it is he who decides when to “go public”
      2. **Emotional release**: Relaxation that is required from the pressure of playing social roles; protection from minor non-compliance with social norms
      3. **Limited and Protected Communication**: Provides individuals with the opportunities needed for sharing confidence and intimacies with those he trusts; allows individuals to seek objective professional advice and not have it used against him
      4. **Self-evaluation**
   3. Legislators would not jump to Westin’s conception of policy due to countervailing interest in costs of providing protection, and bc we don’t people completely control their privacy
2. Cate recognizes 9 Modern Elements of Privacy
   1. **Intrusion**: More electronic based, not necessarily physical
   2. **Discrimination**: Very subtle, though information may be true and relevant, individual’s do not want the information used to harm them
   3. **Embarrassment**: Individuals do not want to be viewed in a vulnerable state; embarrassment is true and not debilitating and not necessarily harmful
   4. **Appropriation**: Against the idea of individuals profiting off of our data; items such as shopping value cards are less privacy intrusive because of choice, value to the consumer
   5. **Fear of manipulation**: Targeted advertising manipulates through provoking our interests
   6. **Deception**: Individuals do not want to be deceived in the way our information is used
   7. **Direct Harm**: Concern that information will be used in a way to cause us injury; ubiquitous data is terrifying to certain people because it puts them at risk of direct, immediate harm
   8. **Government Surveillance**: Unique to the American psyche; Something troubling over the government surveilling us even if we did nothing wrong (may even accrue to our benefit)
   9. **Bureaucracy** (w/ Dan Solove): Fear of being trapped in bureaucratic mindlessness and fail to receive what you are supposed to get; Perhaps not ultimately harmed, but fear over the mind numbing cycle it takes to have issues fixed
3. Additional Perspectives
   1. Julie Cohen, *Examined Lives: Informational Privacy & the Subject as Object*
      1. **Privacy & Respect for Persons**: Purpose of privacy as promoting the development of autonomous individuals and, more broadly, civil society
   2. Daniel Solove, *Conceptualizing Privacy*
      1. **Context**: Contends that the meaning depends upon context, that there is no common denominator to all things we refer to as “privacy”
      2. Norms of privacy vary considerably from place to place, culture to culture, period to period
   3. Anita Allen, *Coercing Privacy*
      1. **Privacy as an inalienable right**: People regularly surrender their privacy and we should “coerce” privacy. Privacy must be seen as an inalienable right, on that people cannot give away
      2. **Eroding Expectations of Privacy:** Society is changing by becoming more exhibitionistic and voyeuristic. Result is that expectations of privacy are eroding
   4. Paul Schwartz, *Privacy and Democracy in Cyberspace* 
      1. **Privacy & Personhood**: Privacy is essential for self-development, and a functional democratic society, cbilitoy to control use of one’s data
      2. **Criticizes Conception of Privacy as Control over Information**: Right to keep data isolated is illusory due to demands of the information age (data seclusion deception); Individuals can be trapped when glorification of freedom of action neglects the actual conditions of a choice (autonomy trap)
   5. Spiros Simitis, *Reviewing Privacy in an Information Society* 
      1. **Privacy and Democracy**: This relationship makes clear the necessity to secure individual’s ability to communicate and participate.
      2. Regulations that create precisely specified conditions for personal data processing are the decisive test for discerning whether society is aware of this price and willing to pay it
   6. Federal Trade Commission
      1. Main focus of privacy policies is that the consumer has notice that allows them to exercise a meaningful choice
      2. Without notice, consumer cannot make a meaningful decision whether to disclose personal information
4. Critics of Privacy
   1. Amitai Etzioni, *Limits of Privacy*
      1. **Privacy & the Common Good**: Privacy is in tension with the common good
      2. Publicness reduces the need for public control, while excessive privacy often necessitates state-imposed limits on private choices
      3. Strengthening the community will further privacy
   2. Richard Posner, *The Right to Privacy*
      1. **Economic Conception**: Everyone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representation (implicit or explicit) that those individuals make concerning their moral qualities
      2. Much of the demand for privacy concerns discreditable informational variance with a person’s professed moral standards, meant to mislead those w/ whom he transacts
   3. Fred Cate, *Principles of Internet Privacy*
      1. **Free Flow of Information**: Free flows of information create a democratization of opportunity in the United States
      2. Part of the equality at the basis of American life concerns economic opportunity, and a certain kind of flow of personal info will contribute to that goal
5. Problem in defining privacy as Control
   1. There are people or settings where we do not want individual privacy control exercised
      1. Financial records, criminal history, etc…
   2. Instances exist where there are head on conflicts over the right
      1. Legal disciplinary proceedings; doctors reporting infection rates
   3. Control may either be non-existent or too costly to provide those opportunities
      1. Ex. Cloud storage, storing info where we do not know where it is geographically located; difficult to control information in centralized systems
   4. Amount of individual data grows logarithmically, difficulty in determining how granular we want control to be
      1. Due to historical founding, most privacy protection focused only on government, and the single place where choice is least workable is in a government setting
   5. Involves a political choice
      1. Control based laws created a bright line system that either provides protection if you qualify, or none at all if you do not
      2. These qualification decisions have huge implications for the public at large

II. PRIVACY AND THE PUBLIC SECTOR

***A. Fourth Amendment and Emerging Technology***

I. Overview of Privacy and Law Enforcement

1. Privacy and Security
   1. Throughout the 20th century, technology provided the government significantly greater ability to probe into the private lives of individuals
   2. Prevailing metaphor is Orwell’s, *1984*, and the depiction of “big brother” watching
2. 4th & 5th Amendments
   1. Constitution provides a national regulatory regime for police conduct, where 4th and 5th amendments significantly limit government’s power to collect information
   2. 4th Amendment: “The right of the people to be **secure** in their persons, houses, papers, and effects, against unreasonable searches and seizures”
      1. Overriding function is to protect personal privacy and dignity against unwarranted intrusion by the state (*Schmerber v. California*)
      2. Only searches and seizure that are regulated are unreasonable ones, if they are reasonable, government has rights to proceed
      3. Search is unreasonable if it is not based on warrant issued by an independent magistrate, before government intrudes into a private space, should have authorization from a separate power (judicial branch, separate from the police)
   3. 5th Amendment: Privilege against self incrimination – “No person shall be compelled in any criminal case to be a witness against himself”
      1. Prohibits the government from compelling individuals to disclose inculpatory information about themselves
      2. Does not apply to all incrimination statements, but to information that is compelled, incriminating, and “testimonial” in nature
         1. Does not protect broadly against prying into private secrets
      3. Does **not apply** to fingerprinting, photographing, measurements, writing of speaking for identification purposes, and having blood or bodily fluids drawn and tested (*Schmerber v. California*)
3. Privacy of the Mail
   1. *Ex Parte Jackson*: 4th amendment required a warrant to search the **contents of sealed letters** sent via the USPS; Does **not protect the outside of letters**, where addressing of information is typically located
      1. Federal law also restricts government’s ability to search mail of **domestic origin**
   2. Government can search letters sent from abroad (*US v. Various Article of Obscene Merch*)
4. Privacy of Papers & Documents
   1. **Mere Evidence Rule** (now defunct): Government could only seize papers if they were instrumentalities of a crime, fruits of a crime, or illegal contraband
      1. *Boyd v. US*: Where government issued a subpoena to compel Boyd, a merchant, to produce invoices on cases of imported glass for use in a civil forfeiture proceeding, the subpoena violated both the 4th and 5th amendment
      2. *Gouled v. US*: Law enforcement could not use search warrants to search a person’s “house or office or papers” to obtain evidence to sue against her in a criminal proceeding
   2. *Warden v. Hayden* **abolished the Mere Evidence rule**
      1. Under the 5th amendment, government can require a person to produce papers and records of a certain character;
         1. e.g., public records or records required by law to be kept; where duty to do so is voluntarily assumed, overriding privilege (*Shapiro*)
      2. 5th Amendment does not protect against subpoenas for a person’s records and papers held by third parties
   3. The 5th Amendment is not a general protector of privacy, but protects against the compelled self-incrimination
      1. Only prevents inquisitorial pressure or coercion against a potentially accused person, compelling her against her will to utter self-condemnation or produce incriminating documents
      2. 5th amendment is a personal privilege, adheres basically to the person, no tot information that may incriminate him
5. Applicability of the 4th Amendment
   1. 4th Amendment governs the investigatory power of government officials, and applies every time a government official conducts a search or seizure of an object or document
      1. Seizure can be of physical things or of persons (arrests)
      2. There must be a search or seizure to invoke 4th amendment protection
   2. Courts seem to withhold constitutional protection from aspects that individuals openly share or knowingly expose to the public (just one other person)
      1. Vehicles are able to be searched with a lower standard than probable cause, as it is not held to the same standard of the home, but it is not totally public (inbetween)
   3. **“Plain View” Exception**: 4th Amendment does not apply to whatever law enforcement officials observe in plain view (assuming they have a legal right to be on the premises, or are in areas impliedly open to the public)
   4. **“Special Needs” Exception**: Searches and seizures are **reasonable without a warrant or probable cause** if “special needs, beyond the normal need for law enforcement make the warrant and probable-cause requirement impracticable”
      1. Validity of a search is judged by the standard of reasonableness under a totality of the circumstances
      2. A**pplies only when a search is not for a law enforcement purpose**, as opposed to searches that might be conducted in conjunction with or at the behest of law enforcement officials
   5. **Exigent Circumstances**: Where circumstances are so unusual, or clearly evident that the search was not unreasonable given the totality of the circumstances (e.g., hot pursuit, imminent destruction of evidence, emergency care)
   6. **“Terry Stop” Exception**: Police officer can stop an individual if the officer has reasonable suspicion that criminal activity is afoot (*Terry v. Ohio*)
      1. Standard is lower than probable cause
      2. The stop must be brief or temporary, if it lasts too long it becomes a seizure, which requires probable cause
         1. Officer may frisk an individual for weapons if the officer has reasonable suspicion that person is armed and dangerous (frisk is not a full search)
      3. Officer cannot search for anything else, only weapons
         1. If in the course of search a person for weapons, the officer finds evidence of a crime, it will still be admissible it found within the scope of a valid frisk
         2. If officer feels something, doesn’t reasonably believe it to be a weapon, but inspects it anyway, that is an unconstitutional search and seizure
6. Administrative Searches
   1. Generally, the need to inspect homes for health and safety violations is outweighed by the individual’s privacy interest
   2. *Camara v. Municipal Ct*: Warrantless inspections of residence for housing code violations were unreasonable
7. Checkpoints
   1. Law enforcement cannot randomly stop cars to check license and regulation, however, fixed sobriety checkpoints are constitutional
      1. DUI checkpoints are a mini incursion on privacy, and involves a good public purpose intrinsically related to driving, thus imposing this burden on drivers fits within a logical nexus
      2. Reasonable expectation of privacy exists w/in a car, not the exterior of a car
      3. Generally, seizure must be accompanied by some measure of individual suspicion
   2. *Indianapolis v. Edmond*: Checkpoints established to investigate possible drug violations were indistinguishable from a general purpose crime control search and were therefore unconstitutional
      1. “General interest in crime control” is not a justification for suscpicionless stops
      2. When primary purpose of the checkpoint is to uncover evidence of ordinary criminal wrong doing, program contravenes the 4th amendment
      3. More intrusive and not intrinsically related to driving, carrying drugs does not make you a bad driver, where being drunk does
      4. If someone is pulled over for drunk driving, and drugs are observed in plain view, that is an arrestable drug offense
   3. Special law enforcement concerns will sometimes justify highways stops without individualized suspicion (*Illinois v. Lidster*)
      1. Relevant public concern was grave
      2. The traffic stop advanced the grave public concern to a significant degree
      3. Most importantly, stops interfered only minimally with liberty of the sort the 4th amendment seeks to protect
         1. Stops only lasted a few seconds, subjectively, contact provided little reason for anxiety or alarm
   4. ***MacWade v. Kelly***: NYPD instituted a random search program for bags and items entering the subway station, in the face of a subway bombing in London; Court upheld the program under a 4th Amendment challenge
      1. Subway rider enjoys full privacy in contents of baggage, but search at issue here minimally intrudes upon that interest as the program is narrowly tailored to achieve its purpose (239)
      2. Program is a reasonable effective means of addressing the government interest in deterring and detecting a terrorist attack on the subway
         1. This is under rational level scrutiny, no argument for privacy rights
         2. This is the classic problem of a privacy case
8. Redress for Law Enforcement Violation of Individual’s 4th Amendment rights
   1. **Exclusionary Rule**: If the individual is a defendant in a criminal trial, the evidence obtained in violation of the 4th amendment can be suppressed
      1. **Fruit of the Poisonous Tree**: If the police illegally search or seize evidence in violation of the constitution, not only is that evidence suppressed, but all other evidence derived from the illegally obtained evidence is also suppressed
      2. If the police obtained a warrant or located evidence by an independent source, fruit of the poisonous tree doctrine does not apply
   2. **Civil Remedy**: Person can obtain civil damages for a 4th amendment violation under 42 USC §1983

II. Wiretapping, Bugging, and Beyond

1. Binary perspective of Reasonable Search and Seizure
   1. Reasonableness of probable cause (warrant aspect of the equation)
   2. The standard for a reasonable expectation of privacy
2. Electronic Surveillance under the 4th Amendment: *Olmstead v. US*
   1. **Physical Trespass Doctrine**: 4th Amendment protections are triggered only when there is a physical trespass into the home (wiretapping here)
      1. 4th amendment cannot be extended and expanded to include telephone wires, or other aspects reaching to the whole world from defendant’s home or office
   2. **Distinguished** from *Silverman v. US*, where police used a spike mike placed in a wall adjoined to the target home to listen to conversations
      1. SCOTUS said that this method usurped part of the defendant’s house or office and constituted unauthorized physical encroachment, and unconstitutional
   3. Dissent contends that protection under 4th amendment is broader in scope, and constitution needs to keep pace with evolving technology
3. Bugs, Transmitter, and Recording Devices: ***Lopez v. US***
   1. **Misplaced Trust Doctrine:** No 4th Amendment Violation when people place their trust in other at their own peril and must assume the risk of betrayal
      1. When he was being recorded, individual was confidentially and indiscreetly talking with someone he trusted, and was just overheard
      2. Same effect on privacy as if agent had been eavesdropping outside an open window
      3. Use of glasses or telescope to magnify the object of a witness’ vision is not forbidden search or seizure, even w/o knowledge or consent as to what someone assumes is private indiscretions
   2. The assumed risk in illicit behavior includes the risk that the conversation would be accurately reproduce in court, whether by faultless memory or mechanical recording
      1. But a plain recording (not through some 3rd party, direct recording) is implicitly unconstitutional under the 4th amendment
4. Reasonable Expectation of Privacy: ***Katz v. US***
   1. What a person knowingly exposes to the public, even in his own home or office, is not subject to 4th amendment protection, **but** what he seeks to keep private, even in an area accessible to the public, is subject to constitutional protection
      1. SCOTUS says 4th amendment protects people, not places
      2. Phone booth was wiretapped in this case, and was found an unreasonable search (physical intrusion was not necessary)
      3. Essentially overturns *Olmstead’s* physical trespass doctrine
   2. **“Reasonable Expectation of Privacy” Test** (Harlan’s Concurrence)
      1. Person must exhibit an actual (subjective) expectation of privacy
         1. If a person believes they have an expectation of privacy this prong is fulfilled; Thus, courts only concerned about 2nd prong
      2. The expectation must be one that society is prepare to recognize as reasonable
         1. In most circumstances, societal expectations do not match the court’s
         2. Reasonableness is evaluated after the fact, so unable to establish what the objectively private expectation is until someone is tried
         3. Ignores individual differences, done by a nationwide reasonable person standard
         4. This standard is rarely found by courts, denies rights of individual defendants in favor of general rights
   3. Courts are in charge of establishing this reasonable expectation standard
      1. Because privacy rights are raised most often by guilty defendants, not a good class to be raising these privacy rights issues in front of the courts
5. What Expectations are Constitutionally Justifiable under *Katz*: *US v. White*
   1. If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered as evidence
      1. Here, government agents who testified about conversations between the defendant and an informant which the agents overheard by monitoring the frequency of a radio transmitter carried by Jackson and concealed on his person
      2. Differs from *Lopez*, in that officers heard the conversation simultaneously, not on a later recording
      3. Misplaced trust doctrine lives on, even after *Katz*
   2. Defendant who has no constitutional right to exclude the informer’s unaided testimony has no fourth amendment privilege against a more accurate version of the events

III. Reasonable Expectation of Privacy Test and Emerging Technology

1. Applying the Reasonable Expectation of Privacy Test: *Smith v. Maryland*
   1. Pen register records outgoing phone calls; Trap and trace device records all incoming call
      1. SCOTUS holds that a use of pen registers or trap and trace was not a form of wiretap (akin to *Katz*, where it was unconstitutional)
      2. Can keep secrets from the government (unless they have a warrant), but not anything else
   2. Does defendant have a subjective expectation of privacy (differences from *Katz* wiretap)
      1. Unreasonable to believe that outgoing numbers should be held private
      2. When using a telephone, information is exposed to phone company equipment during ordinary business; assumed risk of volunteering info to a 3rd party
      3. Constitutionally, government is free to collect any number or information voluntarily turned over to a third party (**3rd Party Doctrine**, *see US v. Miller*)
   3. Congress reacted to *Smith* by enacting the Pen Register Act (18 USC §§3121-3127)
      1. Requires that the government obtain an order certifying that the use of the device is relevant to an ongoing investigation
      2. Less stringent standard then probable cause under the 4th Amendment
2. Dog Sniff Cases Generally: *US v. Place* 
   1. Drug sniffing dogs do **not** constitute a search
      1. Person possesses a privacy interest in the contents of personal luggage under the 4th amendment, but a dog sniff by a trained dog does not require opening the luggage
   2. Dog sniff is *sui generis*, discloses only the presence or absence of contraband
      1. Exposure of an individual’s luggage, located in a public place, to a trained canine is not a search under the 4th amendment
      2. If trained dog approaches your luggage and starts sniffing and barking, probable cause for a warrant is established
3. No Legitimate Interests in Privacy: ***Illinois v. Caballes***
   1. 4th Amendment does **not** require reasonable, articulable suspicion to justify a drug-detection dog to sniff a vehicle during a legitimate traffic stop
      1. Official conduct that does not compromise any legitimate interest in privacy is not a search subject to the 4th amendment
   2. Dog sniff is *sui generus*, when it is properly conducted, the sniff generally only reveals the presence of contraband
      1. Any interest in possessing contraband cannot be deemed legitimate, and thus, government conduct that **only reveals the possession of contraband** (and explicitly nothing else) compromises no legitimate privacy interest (SCOTUS finds inaccuracy irrelevant here)
      2. Even if dog barks (and is ultimately wrong), officers are allowed to search and plain view doctrine then applies
4. No Subjective Expectation of Privacy (that is objectively reasonable): ***CA v. Greenwood***
   1. An expectation of privacy does not give rise to 4th amendment protection unless society accepts that expectation as objectively reasonable
   2. Any privacy interest (in garbage) is waived when you have shown intention to discard it, defeating any claim to 4th amendment protection
      1. Common knowledge that garbage left on a public street is readily accessible
      2. Placing refuse on the curb for the express purpose of conveying it to a third party (Trash collector) negates any public interest (**3rd party doctrine**)
         1. Essentially, police could look through trash after it was dumped somewhere, hence they can go through trash once it is abandoned
   3. Court holds a generous view as to what is considered “not private” and “not triggering 4th amendment protection”
      1. Dissent argues that it is common sense and public decency that you are not supposed to go through other people’s trash
5. Plain View, Open Fields, and Curtilage
   1. **Plain View**: If it is possible for something to be seen or heard from a public vantage point, there is no reasonable expectation of privacy
   2. **Open Fields**: Individual does not have a reasonable expectation of privacy in the open fields that she owns (e.g., farms), even when attempting to keep them secluded and shielded from public view or when it is beyond plain view
      1. Not limited to aerial searches, even if officers trespass, in an open field there is no reasonable expectation of privacy
      2. *Oliver v. US*: police trespassed on the open field, but court found it constitutional
   3. Exception to OFD; “**Curtilage**”: Parts of one’s property immediately outside one’s home do not fall within open field rule, undergoes consideration for 4th amendment protection
      1. No automatic 4th amendment protection
      2. Depends on whether the area in question is so intimately tied to the home itself that it should be placed under home’s umbrella of protection under the 4th amendment
6. Extension of Open Fields Doctrine (Aerially): *Florida v. Riley* 
   1. What a person knowingly exposes to the public, even in his own home or office is not subject to 4th Amendment protection
      1. Because area fell w/in curtilage of the home, and he fenced off the property and posted “do not enter signs,” there was reasonable expectation of privacy against ground-level observation
   2. Because the sides and roof of his greenhouse were left partially open, the contents of the greenhouse were subject to viewing from the air
      1. **Cannot reasonably have expected the contents of the greenhouse to be immune from examination by an officer in an aircraft flying in navigable airspace**
      2. Private and commercial flight (by helicopter) in the public airways is routine, and no indication that such fights are unheard of in this area
   3. No reasonable expectation that green house was protected from public or official observation from a helicopter as long as it is flying within navigable airspace for the type of aircraft it is (cites *California v. Ciraolo*)
      1. Dissent argues that this is machinery that few ordinary citizens have, thus it impinges on a reasonable expectation of privacy
7. Sensory Enhancement Technology: ***Dow Chemical v. US***
   1. Dow has a reasonable, legitimate and objective expectation of privacy within the interior of its covered buildings
      1. Cannot be expected that Dow erect a cover over a 2,000 acre tract, however its exposed manufacturing facilities are not analogous to curtilage surrounding a home, even if it took steps to bar access from ground level
      2. Intimate activities associate with family privacy and home and curtilage do not reach outdoor areas between structures of a manufacturing plant
      3. Curtilage exception applies only to private real estate, not commercial property
   2. Though the photos taking give the EPA more detailed information than a naked eye view, the mere fact that human vision is enhanced somewhat (at least to the degree here – outlines of building facilities and equipment) does not raise constitutional problems
      1. Taking aerial photos of an industrial plant complex from navigable airspace is not a 4th amendment prohibited search
      2. Surveillance by highly sophisticated equipment generally not available to the public and uncovering confidential information is a different situation
8. Thermal Image Technology and the Right of Your Own Home: ***Kyllo v. US***
   1. Core of the 4th amendment right is that of a man to retreat to his very own home
      1. Where government uses a **device that is** **not in general public use**, to explore details of the home that would previously have been unknowable without physical intrusion, **surveillance is a search and unconstitutional** without a warrant
   2. Does not indicate whether the technology allows us to see through the wall, or just to observe that a wall is merely heated
      1. SCOTUS comes to decision without any proof or demonstration of this question
      2. Focuses on technology by government that was not in public use
   3. Reconciling *Kyllo* with *Cabelles* (drug sniffing dogs)
      1. Distinction is that, in *Kyllo*, the device was able to detect lawful activities (such as saunas or bath – thermal imaging focuses solely on heat), where drug sniffing dogs only detect contraband
      2. Legitimate expectation that info about perfectly lawful activity will remain private is categorically distinguishable from hopes or expectations concerning non-detection of contraband in a car trunk
      3. *Kyllo* decision directly related to the right for individuals to retreat to their own homes, as the technology revealed something about what goes on in a private home, besides illegal activity (unlike in a dog sniff)
9. Scope of the Right to Privacy
   1. 4th Amendment only acts as a restraint on a collection of information, not the use of information (unless exclusionary rule is applied)
      1. Protection applies to search and seizures, not the sharing, distribution, or use of private information
      2. Imposes no restraint on what government does with information that it already has
      3. Cannot raise a 4th amendment claim if government uses info in a way you don’t like
   2. Bc there is no constitutional provision related to use of data, even if the government collects data illegally, it can use that information for whatever purpose it wishes, with the exception of the exclusionary rule
      1. Though information may be excluded in situation where it was obtained illegally in that specific proceeding, the government is still free to use it in non-related settings
      2. Ex. Information obtained illegally for criminal trial is excluded, however, if tax court wants to raise separate action, it can use that illegally obtained information
      3. 4th amendment is limited in privacy protection, because it is limited in how it applies, only to data collection
      4. If information is collected lawfully, information can be used for any subsequent purpose, obviously
   3. No reasonable Expectation of Privacy Exists
      1. Information exposed to someone else
      2. Observable in plain view
      3. Located in an open field (even without plain view)
      4. Aerial search (except for curtilage of a home; no extension to commercial prop)

***B. Government Access to Private Sector Records***

I. Information Gathering Without Search Warrants

1. Subpoenas
   1. *Fisher v. United States* expanded holding in *Couch* (where tax records could be subpoenaed w/o violation the 4th or 5th amendments) to include disclosure of nearly all private papers
   2. Later cases cut back on the breadth of *Fisher*, holding that the act of a party producing a document **can** constitute a 5th amendment violation, however most subpoenas seeking personal papers are directed at third parties
2. 4th Amendment Protection to Information Held by 3rd Parties: *Gonzales v. Google*
   1. Government sought a listing of the text of all search queries entered into Google over a two month period
   2. District Court held, even if an expectation by Google users that Google would prevent disclosure to the government of its users’ search queries is not entirely reasonable, but information indicates at least some users expect some privacy in their searches
      1. Expectation may not be reasonable, but nonetheless have an appreciable impact in which Google is perceived, and consequently the frequency with which it is used
      2. Expectation does not rise to absolute privilege, but does indicate that there is potential burden as to loss of goodwill if forced to disclose search queries
3. Bank Secrecy Act
   1. Federal obligation that banks keep certain records about their customers and provide that information to government, systematically or upon request
   2. Anti-Privacy Statute: If you offer financial services regulated by the government, required to comply with this act
      1. Effectively, all customers of financial institutions must have identities verified and kept on file for length of account and a period of time afterwards
      2. All transactional records must be retained for some time (ATM, etc…)
      3. If a transaction exceeds $10,000, must be reported to federal government
         1. For international transfers, threshold is $5,000
      4. Financial institutions of any kind must file SAR’s (suspicion activity reports) dealing with suspicious parties and abnormally large amounts
         1. Over 75 millions SAR’s filed in the past decade
4. Right to Privacy and the Bank Secrecy Act: ***CA Bankers Ass’n v. Shultz***
   1. SCOTUS held that the Act did not violate the 4th amendment because bankers did not possess 4th amendment rights in the information
      1. Corporations are not equal w/ individuals in the enjoyment of a right to privacy
   2. General v. Specific Searches
      1. 4th amendment primarily protects general searches; must be reasonable, and conducted with probable cause; judicial oversight exists in this process
      2. Dissent argues that the ability to review everyone’s financial transactions in order to ferret out criminal activity resembles a general search
      3. Dissent says that this assumes that every citizen is a criminal; Takes a sledgehammer approach, when it should approach delicately with a scalpel
5. Third Party Doctrine**: *US. v. Miller*** 
   1. **Third Party Doctrine** states that data disclosed or held by a third party is no longer subject to any 4th amendment protection as to a right to privacy
      1. *Katz* stresses that what a person knowingly exposes to the public is not subject to 4th amendment protections
      2. Checks and financial materials are exposed to someone else (bank tellers, etc…), thus there is no legitimate expectation of privacy
   2. Privacy depends entirely on the location of information/documents
      1. If an individual is in sole possession, right to privacy exists
      2. If someone else also has access, it is not protected
   3. Circumstances of case applied
      1. Two banks were subpoenaed and presented records relating to the criminal defendant that were produced in accordance with the Bank Secrecy Act
         1. Records were not at Miller’s home, they were stored at the bank (thus only the subpoena was necessary)
         2. Information gathered here are not Miller’s private records, and records of the bank secrecy act do not violate anyone’s privacy
      2. Even if information is revealed on the basis of an assumption that it is only for a limited purpose and that confidence placed in the third party will not be betrayed, no 4th amendment right to privacy exists
   4. Congress enacts **Right to Financial Privacy Act** in response to *Miller*
      1. Prevents banks and other financial institutions from disclosing a person’s financial information to the government unless the records are disclosed pursuant to subpoena or search warrant (29 USC §§3401-3422)
6. Effect of *Miller* and the 3rd Party Doctrine
   1. Courts have established that even if the government is using a 3rd party as an instrument of the government, requiring systems to keep data about customers for the sole purpose of obtaining information w/o violation the 4th amendment is allowable
   2. Court views privacy in terms of secrecy and confidentiality, if anyone knows of the information it cannot considered private
   3. In the FOIA context however, public records can be found as private; privacy is found by the government in the narrowest of aspects

II. Information Gathering with Search Warrants

1. 1st Amendment and the Right to Privacy: *Zurcher v. Stanford Daily* 
   1. Properly administered, the preconditions for a warrant (probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness) should afford sufficient protection against the harms that are assertedly threatened by warrants for searching news paper offices
   2. Prior cases do no more than insist that the courts apply the warrant requirements with particular exactitude when 1st amendment interests would be endangered by the search
      1. Where presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field
   3. Under the 4th amendment, a search warrant may be issued if there is probable cause to believe that incriminating evidence is in the place to be searched
      1. This is not limited to places owned or occupied by the criminal suspect, even after considering tension between the press and the crown, newspaper offices can be searched as a “third party” as long as it is properly conducted with no violations of either the 1st or 4th amendment
2. Privacy Protection Act
   1. Passed in 1980 by congress in response to *Zurcher* 
      1. Effectively requires law enforcement to obtain a subpoena in order to obtain such information
      2. Unlike search warrants, allows a party subject to them to challenge them in court before having to comply, and the person served with the subpoena must produce documents themselves (rather than law enforcement searching through records)
   2. Unlawful for a government official to search or seize any work product possessed by a person reasonably believed to have a purpose to disseminate public communication in connection with investigation or prosecution of a criminal offense
      1. If probable cause exists that the person possessing such materials has committed or is committing a crime to which the materials relate, they can be searched or seized
      2. Criminal offense cannot consist of the mere receipt, possession or communication of the materials
      3. Materials may be searched or seized if reason to believe that the immediate seizure is needed to prevent death or serious bodily injury
   3. PPA also applies to restricting search or seizure of documentary materials, other than work product, possessed by a person in connection with a purpose to disseminate public communication

***C. Constitutional Protection of Medical Information in the Public Sector***

I. Constitutional Right to Privacy

1. U.S. Constitution does not explicitly mention privacy
   1. Under substantive due process, SCOTUS held that there exists a “right to privacy” in the U.S. constitution
2. Substantive Due Process Right to Privacy: Griswold v. Connecticut
   1. Specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees; Various guarantees create **zones of privacy**
      1. 1st, 3rd, 4th, 5th, 9th amendments form these zones of privacy
   2. Criminalization of contraceptives and the counseling about contraceptives falls within the zone of privacy created by several fundamental constitutional guarantees
      1. Concern over government access to information, albeit about a specially protected relationship in a specially protected place
      2. Decision driven by fear of government intrusion into both physical and social private zone in pursuit of information
   3. Government purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broad and thereby invade area of protected freedoms

II. Constitutional Right to Information Privacy

1. Constitutional Right to Info-Privacy: ***Whalen v. Roe***
   1. *Whalen* is the first constitutional challenge that goes to the issue of collecting data
      1. Right to Informational Privacy is another operational right to privacy (beyond the 4th amendment), however does not have much control at this point
   2. Characterized the line of substantive due process (14th amendment) cases protecting the right of privacy as involving two “different kinds of interests”
      1. **Constitutional Right to Information Privacy**:
         1. The individual interest in avoiding disclosure of information about a fundamental interest
         2. Privacy implications of the collection, use, and disclosure of personal information
         3. Has not been used by SCOTUS to strike down any action (whereas decisional privacy has been used to strike government restraints)
      2. **Decisional Privacy**:
         1. The interest in independence in making certain kinds of important decisions, applies only to fundamental rights
         2. Involves extent to which the state can become involved with the decisions an individual makes with regard to her body and family
   3. In this case, court held that while informational privacy rights are implicated, there is no violation in a statute that requires physicians to report prescription information concerning certain protected narcotics
      1. Implication of fundamental right: Some individuals would be discouraged to receive drugs because they did not want state to receive information, so that the state may raise some inference or have information leaked
         1. Individual interest in avoiding disclosure of personal matters
         2. Interest in independence in making certain kinds of important decisions
      2. Court cites legislatively imposed sanctions and legislatively required security protections to establish no violation of the constitutional info privacy right
   4. Response by Judicial Circuits
      1. Some circuits use the new informational privacy requirements to strike down certain government disclosure requirements (under intermediate scrutiny)
         1. Decisional privacy is evaluated under strict scrutiny
      2. Other circuits viewed the requirements as not offering much protection
2. Deciding Whether Constitutional Right to Informational Privacy Exists: *US v. Westinghouse*
   1. **Westinghouse Test**: 7 factors to determine whether a given disclosure constitutes an actionable invasion of privacy
      1. Type of record requested
      2. Information it does or might contain
      3. Potential for harm in any subsequent nonconsensual disclosure
      4. Injury from disclosure to the relationship in which the record was generated
      5. Adequacy of safeguards to prevent unauthorized disclosure
      6. Degree of need for access
      7. Whether there is an express statutory mandate, public policy, or other recognizable public interest militating toward access
3. 42 USC §1983 Claims & Constitutional Torts
   1. Most cases involving the constitutional right to info privacy are §1983 claims
      1. Enforcement of civil rights protected by constitution and federal law
   2. Remedies constitutional violation in the civil context, creating a cause of action against state governmental authority that violates federal law and the constitution
      1. Requires that the wrongful conduct be under color of state law, custom, or usage
      2. Any state or local official can be sued directly under §1983
      3. State government cannot be sued, but local governments can (but only when their policy or custom inflicts the injury, not bc they employ officials who caused injury)
      4. §1983 does not authorize suits against federal officials, however SCOTUS held in *Bivens* that federal officials can be sued for violating constitutional rights, and are addressed in a similar way as §1983 claims
   3. 2 Scenarios exist (Get one or the other, not both)
      1. Court acknowledges that a recognized right should exist, and notifies government that if they violate this in the future, charges will be pressed
      2. Court recognizes the right already exists and press charges
4. §1983 Claim for Violation of Constitutional Right to Info-Privacy: ***Doe v. Borough of Barrington***
   1. Federal constitutional right that §1983 claims is based upon is their right to privacy under substantive due process of the 14th Amendment
      1. *Whalen* demonstrates that, not only is the government restricted from collecting personal medical information, it may be restricted from disclosing such private information it lawfully receives
   2. Privacy interest in medical information and records is not absolute, court must determine whether the societal interest in disclosure outweighs the privacy interest involved
      1. To avoid a constitutional violation, government must show a compelling state interest in breach that privacy
   3. Here, officer did not advance a compelling government interest in preventing spread of HIV, because there was no risk that those he disclosed the information to would be exposed to the virus through casual contact (medically established, and well known)
      1. Right to privacy of an individual’s AIDS diagnoses extends to members of the patient’s immediate family
   4. Standing Issue: Argument that disclosure only affects Mr. Doe, not his wife or kids
      1. Family member’s diagnoses of AIDS is a **personal matter** that implicates the entire family, and falls within constitutional protection
      2. **Stigma** attaches to all family members, whether or not they have the disease (this took place at time when AIDS was an unknown)
5. Insufficient Privacy Concerns for a Constitutional Violation: ***Doe v. SE Penn. Trans. Authority***
   1. It is nearly impossible to recover under a privacy claim, why an individual discloses that identifiable information themselves
      1. Here, Doe disclosed his HIV diagnoses to the staff physician
      2. Personal disclosure of information does not give other co-workers cart blanch to invade his privacy (other here, found out the condition independently)
   2. No harm was incurred by Doe here
      1. Had ER took adverse action against him, or disclosed it to other EE’s so they could take appropriate action, claim would be more legitimate, but not dispositive
   3. Individual using prescription drugs has a right to expect that such info will customarily remain private, however, it must be balanced against important competing interest
      1. ER’s legitimate need for this information may affect whether disclosure is an actionable one
      2. ER has a right to ensure health plans are being used by those who are authorized to be covered, and to accomplish theses goals, ER’s must have access to reports from suppliers, and they must inspect them
   4. When information disclosed is only for the purpose of monitoring plan by those with a need to know, EE’s interest in keeping prescription info private is outweighed
      1. Impingements on privacy are insufficient to constitute a constitutional violation if intrusion is minimal as such

III. The Fourth Amendment

1. **“Special Need”** as Justification for Warrantless Search: ***Ferguson v. City of Charleston***
   1. In previous cases where drug testing was upheld as a “special need,” the invasion of privacy was much lower then in this case
      1. Where special needs were upheld, no misunderstanding about the purpose or use of the test, and there were protection against dissemination of results to 3rd parties
      2. Justification for the absence of a warrant or individualized suspicion was one divorced from State’s general interest in law enforcement
   2. Balancing test must weigh intrusion of individual interest in privacy against the “special needs” that support the program
      1. Patient undergoing tests at a hospital has a reasonable expectation of privacy that results will not be shared with nonmedical personnel w/o consent
   3. **Whatever the “special need” may be, the need must be unrelated to law enforcement**
      1. Once law enforcement is involved in the development or application of the testing policy, the exception evaporates and 4th amendment analysis re-applies
      2. Here, though ultimate goal may have been to help women get off drugs, the immediate objective of the drug test (searches) was to generate evidence for law enforcement purposes (to coerce treatment or prosecution)

***D. Federal Electronic Surveillance Laws***

I. Infancy of Federal Electronic Surveillance

1. §605 of the Federal Communications Act
   1. Responding to *Olmstead* (where court said that wiretapping was not a 4th amendment violation), congress passed the FCA
      1. Did not expressly provide for an exclusionary rule, but could not introduce evidence obtained by illegal wiretapping in federal court
   2. States could still use evidence in violation of §605 in state prosecutions, and only applied to wire communications and wiretapping, not to non-wire communication
      1. Bugging was hence not covered
      2. States could continue wiretapping, §605 only applied federally
2. Title III or the “Wiretap Act”
   1. Applied to wiretaps by federal and state officials as well as by private parties
      1. Required federal agents to apply for a warrant before wiretapping
      2. Criminalize private wiretaps
   2. Exception: If any party to the conversation consented to the tap, there was no violation
      1. Excluded wiretaps for national security purposes from any restrictions
      2. National security exception applied to foreign threats, not internal threats

II. Electronic Communications Privacy Act (ECPA)

1. Statutory Structure
   1. Modernized federal wiretap law, amending Title II and including two new acts
      1. Many of the provisions applied not only to government officials, but to private individuals and entities as well
   2. Federal electronic Surveillance law on the domestic side contains three parts:
      1. Wiretap Act (updated Title III)
      2. Stored Communications Act (SCA)
      3. Penn Register Act
2. Types of Communications (Each type protected differently)
   1. Wire Communications: All aural transfers traveling through a wire or a similar medium
      1. Aural transfer is a communication containing the human voice at any point
         1. Voice only needs to be minor part of communication
         2. A communication that once consists of a human voice that has been translated into code is still an aural transfer
      2. Only part of the journey from origin to destination need not take place via wire
      3. Offered the most protection
   2. Oral Communications:
      1. Communication uttered by a person w/ an expectation that it is not subject to interception under circumstances justifying such expectation
      2. Typically intercepted through bugs or other recording/transmitters devices
   3. Electronic Communications: Consists of all non-wire, non-oral communication
      1. Example: Email is electronic communication (as long as it does not have human voice attached to it at some point)
      2. Given the least protection
         1. Exclusionary rule of wire tap act does not apply to electronic communication
3. Wiretap Act
   1. Interceptions, use, or disclosure of any wire, oral, or electronic communication w/o court order and probable cause of crime (past, present or future) is unlawful
      1. Interception must be minimized to avoid sweeping in communications beyond the purpose for which the order was sought
      2. Applies when communications are intercepted contemporaneously with their transmission; Once the communication is completed and stored, wiretap act no longer applies
   2. For a court wiretapping or electronic surveillance order, must establish probable cause that an enumerated crime has, is, or will be committed (super search warrant/4th amendment)
      1. Exclusionary Rule: Any aggrieved person may move to suppress the contents of any wire or oral communication intercepted, or evidence derived therefrom (but no exclusionary rule for electronic communication)
   3. Exceptions:
      1. Act does not apply if one of the parties to the communication consents
         1. No consent exception when interception is carried out for the purpose of committing any crime or tortious act
      2. Communications service provider is permitted to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service
         1. Service providers may intentionally disclose intercepted communications to the proper authorities when criminal activity is afoot
4. Stored Communications Act (SCA)
   1. Whereas communications in transmission are covered by Wiretap Act, communications in electronic storage are protected under the SCA
      1. Forbids disclosure of contents of stored communications by service providers, intentional access without authorization, and exceeding authorization and altering access to a wire or electronic communication
      2. Depending on situation, requires warrant (stored > 180 days, or <180 and no prior notice to subscriber) or subpoena (stored < 180 and prior notice)
   2. SCA has consent exception, and entirely exempts the person or entity providing a wire or electronic communications service
      1. SCA has no exclusionary rule as a remedy
5. Pen Register Act (Focus primarily on telephones)
   1. Pen register is a device which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument from which a wire or electronic communication is transmitted (does not include contents of any communication)
      1. Pen register records numbers dialed from a phone line
      2. Trap and trace records telephone number of incoming calls
   2. Must first obtain a court order to install a pen register/trap and trace
      1. No exclusionary rule for violations, fine and imprisonment is possible
6. Video Surveillance
   1. If the government intercepts a communication consisting of video images (transmission of webcam or an email video clip), then the wiretap act applies
      1. Assuming these communications at some point were aural
   2. If government accesses an individual’s stored video clip, then the SCA applies
   3. Silent video surveillance is not covered under federal electronic surveillance law
      1. However 4th amendment requirements still apply
7. Electronic Surveillance Law and the 4th Amendment
   1. Electronic surveillance law is independent of the 4th amendment
      1. If a search is reasonable under the 4th amendment, ES law may still bar evidence
      2. If search is authorized, 4th amendment could still prohibit a wiretap
   2. Procedure for warrants are more stringent under Wiretap act than under 4th amendment
      1. 4th amendment search warrants are single entry and prompt
      2. Under wiretap act, surveillance can be 24 hours a day and for 30 days

III. Communications Assistance for Law Enforcement Act (CALEA)

1. CALEA requires telecommunication providers to help facilitate the government in executing legally authorized surveillance
   1. Advancement in technology convinced Congress to force telecommunications providers to ensure that the government could continue to monitor electronic communications
2. Requirements
   1. All telecommunications providers must be able to isolate and intercept electronic communications and be able to deliver them to law enforcement personnel
      1. Must be able to single out an individual phone number
      2. Ensures that government can tap communications
   2. Under a safe harbor provision, carriers that comply with accepted industry standards are in compliance with CALEA
3. Limits
   1. Carriers must facilitate authorized communications interceptions and access to call-identifying information in manner that protects the privacy and security of communications and call-identifying information not authorized to be intercepted
   2. Does not apply to information services, such as email and internet access
4. J-Standard (Interim/Trial Use Standard J-STD-025)
   1. Sets for the standard by which carriers can make communications and call-identifying information available to law enforcement officials
   2. Ex. Required carriers to inform LEOs of the nearest antenna tower to a mobile phone user so they could track location of mobile phones
5. Initially this focused only on voice communications
   1. Becomes complicated with VOIP

IV. USA PATRIOT Act

1. Delayed Notice of Search Warrants
   1. Government may delay notice of a search warrant if the court concludes that there is a reasonable cause that immediate notice will create an adverse result
      1. Physical danger, destroying evidence, delayed trial, flight from prosecution
   2. “Sneak and Peek”: Warrants enabling the covert search with delayed notice
2. New Definition of Pen Registers and Trap and Trace Devices
   1. Expanded ECPA’s focus on pen registers and trap and trace devices from applying beyond telephone numbers, to internet addresses, email address information (to and from), and the routing information of a wide spectrum of communication
   2. Person whose communications are subject to this order don’t have to be a criminal suspect
      1. All the government needs to certify is relevance to an investigation

***E. Digital Searches and Seizures***

I. Searching the Contents of Computers

1. Generic Warrants to Search Computers
   1. These types of general classifications (search warrants applying to entire computer system) is acceptable when a more precise description is not possible (*US v. Lacy*)
      1. Search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs (*US v. Hay*)
   2. Not allowed to expand the scope of the search where it would require another warrant
      1. Obtaining a warrant to search computer for record of illegal drugs, and when finding a porn file, beginning to search for similar files – unconstitutional
2. Requirements to Search a Computer
   1. In searching a house, can search anywhere throughout the house as long as it likely contains what you are looking for
   2. If the house contains multiple persons private things – Foot Locker Rule
      1. If one roommate gives consent to a general search, and police come across a locked foot locker, if the consenter establishes that is not her property, officers do not have consent to search the locker
   3. Grey areas:
      1. If the house has two bedrooms, consent from one makes both rooms searchable
      2. If a computer has a password and a roommate does not know it, the roommate cannot consent to a search of the other person’s password protected computer
   4. Once you have authority to search a computer (by warrant or by consent), officers essentially have free reign to search whatever is in it
3. Password Protected Files: ***Trulock v. Freeh***
   1. Two individuals share a computer but maintain separate files protected by password, and they do not know each other’s password and cannot access each other’s files
      1. When one party consents to a search of the computer, they cannot search the other person’s files because they did not consent.
   2. Although one part consents to a general search of the computer as a whole, his authority did not extend to the other party’s password-protected files
4. “Locked” Computers and Authority to Consent: *US v. Andrus* 
   1. In the issue of 3rd party consent in the context of computers, officers knowledge about password protection is an indication of whether a computer is “locked” in the way a footlocker would be, where the targeted individual’s consent would be needed
      1. Officers are not obligated to ask questions about password protection unless the circumstances are ambiguous (they avoided this here)
      2. Court says the password protection is not in plain view, as long as officers do not ask about the computer or even turn it on, they can dismantle as they please
   2. Despite the lack of any affirmative assertion that the consenting party used the computer, and despite the existence of a profile indicating that the other party intended to exclude other household members form computer use, it was objectively reasonable to believe that there was sufficient authority to consent to the search
      1. Consenting party did not say or do anything to indicate lack of ownership or control over the computer when asked for consent to conduct the search

II. Encryption and E-Mails

1. Encryption includes the ability to keep communications secure by concealing the contents of a message; even if it is intercepted, it still remains secure
   1. Messages are translated into “cipher text,” and parties to the communication hold a key to translate the code to the original message
2. Clipper Chip
   1. Federal encryption standard in which the government would retain a copy of the key in a system call “key escrow”
   2. By holding a “spare key,” the government could readily decrypt encrypted communications if it desired (did not go over well)
3. Key Escrow
   1. Providing a decryption key to a 3rd party who would only provide the decryption information to the government if there was a warrant (did not go over well)
4. Current System treats encryption as munitions
   1. Same laws that limit the export of munitions also limit the use of encryptions outside US
   2. Within the US, free to use any encryption you want
      1. NSA is real good at decryption, but still an issue for state and local gov.
5. E-Mail: *Steve Jackson Games v. USSS*
   1. Under ECPA, email messages stored within her ISP waiting to be downloaded is shielded by the weaker provisions of the SCA rather than the stronger protection of the Wiretap Act
   2. Thus cannot get the suppression remedy only available under Title I (Wiretap Act)
6. Open E-Mail
   1. Only in California is there (See 328)
   2. Everywhere else, if an email is opened, it receives a lower standard of protection
7. What Constitutes an Interception?
   1. Electronic communication includes transient electronic storage that is intrinsic to the communication process, and hence interception of an email message in storage is an offense under the wiretap act

III. ISP Records

1. No reasonable expectation of privacy in ISP records: *US v. Hambrick* 
   1. No reasonable expectation of privacy in ISP records due to the 3rd party doctrine
      1. Screen names become linked to your true identity
      2. By entering into agreement to obtain internet access from a provider, he knowingly revealed his name, address, cc $, and telephone number to the provider and its ee’s
   2. Even though government gained information from provider via faulty subpoena, ECPA is not a legislative determinative, and Congress did not provide suppression where a party obtains stored data or transactional records in violation of the SCA
      1. Nothing suggests there was restrictive agreement between defendant and provider that would limit rights of provider to reveal such information to non-governmentals
      2. Where dissemination of info to nongovernment entities is not prohibited, no reasonable expectation of privacy to that information
   3. Court says that this info was freely provided to the ISP and thus no privacy, but Cate says you have a sn for privacy purpose, and ISP needs your real name to charge for the service
2. Court and Statutory Misjoinder on SCA Suppression: *McVeigh v. Cohen*
   1. ECPA allows government to obtain information from an online service provider only if:
      1. It obtains a warrant issued under the FR of criminal procedure; or
      2. It gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question
   2. By soliciting and obtaining over the phone personal info about plaintiff from the provider, government invoked neither of these provision and failed to comply with ECPA
      1. There is no statutory exclusionary remedy for violation of the SCA
      2. Court creates one here, saying where individual rights are violated, information obtained improperly can be suppressed (Cate says this is wrong, court disregarded law and made its own remedy)
   3. Subsequently, in *Freedman v. AOL*, court made it clear that SCA provision created a reciprocal obligation on the government’s conduct to obtain a warrant or the like before requiring disclosure from the internet provider

IV. IP Addresses and URLs

1. Penn Register Statute Applied to IP and Email To/From: *US v. Forrester* 
   1. Mirror ports are constitutionally indistinguishable from surveillance technique of a pen register in *Smith*
      1. Mirror Ports enable the government to learn the to/from addresses of an individuals emails, and the IP addresses of the websites he visits, and the total volume of info sent to or from his account
      2. Court does not decide if computer surveillance is covered by pen register statute, just saying aspects are constitutionally indistinguishable
   2. Reasoning:
      1. Email and internet users, like telephone users in *Smith*, rely on 3rd party equipment in order to engage in communication, and have no expectation of privacy in the information they voluntarily provide to internet service providers
         1. Like phone #s, this info is voluntarily turned over in order to direct the third party’s servers
      2. Email to/from and IP constitute addressing information do not necessarily reveal any more about the underlying contents of communication, like phone #s
         1. Clear line in *Smith* and *Katz* between unprotected addressing info and protected content; contents deserve 4th amendment protection, but the address and size of packages do not
         2. URL, unlike an IP, identifies the particular document within a website a person views, and thus reveals much more info about that person’s internet activity
2. Scope of the Pen Register Act
   1. Prior to the USA Patriot Act, it was undecided whether the Pen Register Act applied to email headers, IP addresses, and URLs
   2. The Patriot Act changes clarified that the Pen Register Act applied beyond phone #s
      1. Included dialing, routing, addressing or signaling information
      2. Email headers easily fit new definition, but ambiguous about IP and URLs
3. Text Messages
   1. *Quon v. Arch Wireless*: Accessing texts constitutes a violation of the SCA bc the messages were stored by the communication service provider as backup protection for the user
   2. 4th Amendment protects text messages communication because they are content information, like email content in *Forrester* (albeit not the header info)
4. ECPA and the Exclusionary Rule
   1. Even if the acquisition of information violated the Pen Register Act, exclusionary rule is not a remedy under the act
   2. In the wiretap act, wire and oral communications are protected with the exclusionary rule, but electronic communications are not
   3. SCA and Pen Register Act have no exclusionary remedies for any type of communication

V. Key Logging Devices

1. *US v. Scarfo*
   1. 4th amendment requires a certain modicum of particularity in the language of the warrant with respect to the areas and items to be searched and/or seized
      1. Officers are constrained from undertaking a boundless and exploratory rummaging through one’s personal property
   2. The Key Logging System (KLS – deciphers passphrases to encrypted files when installed into a computer) recorded keystrokes typed into a keyboard other than the searched for passphrase – no consequence
      1. This does not make the limited search for the passphrase a general exploratory search
      2. Some innocuous items will be cursorily perused in order to determine whether they are among those items to be seized
   3. Law enforcement officers must be afforded the leeway to wade through potential morass of info in the target location to find the particular evidence properly specified in the warrant
      1. No tenant of the 4th amendment prohibits a search merely because it can’t be performed with surgical precision

***F. National Security and Foreign Intelligence***

I. Is National Security Different

1. Distinctions in Electronic Surveillance: The *Keith* Case
   1. *Katz* is the watershed case for electronic surveillance
      1. Establishes that 4th amendment applies for electronic surveillance
      2. Leaves open questions surrounding obligations of government when conducting search or surveillance for purposes other than law enforcement
   2. Criminal investigations regulations under Title III (ECPA)
      1. Necessary to obtain a warrant in the surveillance of crimes unrelated to the national security interest
   3. Domestic security investigations
      1. 4th amendment requires government to issue a warrant when surveillance purpose is outside of law enforcement (domestic security investigation)
      2. Precise requirements for issuing a warrant to investigate domestic security need not be the same as for ECPA criminal surveillance
      3. Government wanted no judicial oversight in national security matters, but recognizes president’s national security powers, but that it must be exercised compatible to the 4th amendment and proper warrant procedure is required
   4. Investigations involving activities of foreign powers and agents
      1. *Keith* only covers domestic aspect of national security and only applies to US citizens that are not agents of a foreign power
      2. SCOTUS did not address issues involving foreign powers and their agents
      3. Circuit courts have concluded at a minimum, no warrant is required by the 4th amendment for foreign intelligence surveillance, as a warrant requirement would unduly frustrate the President’s foreign affairs responsibilities

II. Foreign Intelligence Surveillance Act

1. FISA establishes standards and procedures for use of electronic surveillance to collect foreign intelligence within the US (which *Keith* declined to address)
   1. Designed primarily for intelligence gathering agencies to regulate how they gain general intelligence about foreign powers & agents of foreign powers within the borders of the US
   2. ECPA is designed for domestic law enforcement to govern the gathering of information for criminal investigations involving people in the US
2. Created the Foreign Intelligence Surveillance Court (FISC)
   1. A secret court comprised of 11 federal judges (appointed by chief justice) that authorizes and grants surveillance (court) orders for intelligence gathering purposes
   2. Must go to the court when foreign intelligence gathering is a **significant** **purpose** of the investigation, does not have to be the primary purpose (Prior to the PATRIOT Act, FISA applied when foreign intelligence gathering was THE primary purpose)
3. Basic Requirements
   1. When targeting a US person not acting as an agent of a foreign power, a FISA court order is required for intelligence related surveillance
      1. Traditional probable cause is not required, only required to meet minimization standards and surveillance of the right place
      2. If foreign powers/agents are the only people involved in surveillance, no court order required
   2. Court must find probable cause that the party to be monitored is a foreign power or an agent of a foreign power; unlike ECPA or the 4th amendment not tied to criminal activity
4. Exceptions to FISC’s approval requirement
   1. Communications at issue are exclusively between or among foreign powers (including national or agents of a foreign power)
   2. Form of interception (excluding the phone tap), as long as the signal source stems from the premises of a foreign person or agent of a foreign power
5. Definitions:
   1. **Foreign intelligence**:
      1. Any information about a foreign government, or int’l terrorist threat
      2. Domestic terrorism is included
      3. This is the standard for FISA (law enforcement uses ECPA)
   2. **Foreign Power**: Foreign government, or any component thereof not substantially composed of US persons, that are engaged in int’l terrorism, or a foreign based political organization not composed of US peoples
   3. **Agent**: US and Non-US persons who do certain things
   4. **Int’l Terrorism**:
      1. Violent or dangerous act to human life, property, etc…
      2. Intended to intimidate or coerce civilian population, or effect conduct of gov’t through violence with a purpose
      3. Geographically, int’l terrorism occurs outside the US, or if aims, intimidation, and coercion transcends national boundaries (or seeking asylum or receive aid from another country)
6. FISA Amendments Act (FAA)
   1. Under FAA, NSA allowed to gather mass amounts of data and sort it out later (vacuum)
      1. Post 9/11 FISA does not have jurisdiction over data mining/collection
   2. Effectively allows the AG or Director or National Intelligence to authorize jointly, for up to one year, the targeting of persons reasonably believed to be located outside the US to acquire foreign intelligence information
      1. Does not matter if all or some communication occurs w/in the US
      2. No role for the FISC, only approves minimization procedures
   3. Government may not engage in reverse targeting: Cannot target a person reasonably believed to be outside US, if purpose is to target a known person reasonably within the US
      1. Ex. Cannot circumvent FISA and ECPA to conduct surveillance about Y, knowing that you will get conversation’s with X under the lower standard
      2. Permissible to collect all information and then get X’s communication, but specific targeting is not allowed under ECPA
   4. Granted immunity to telecommunications providers participating in illegal surveillance up to that point where it is not possible in advance to know whether a communication is purely int’l or whether the communication involves a foreign power or its agents
7. Probable Cause for a Warrant under FISA: ***Global Relief Foundation v. O’Neil***
   1. Probable Cause: FISA requires a judicial finding that probable cause exists to believe that the target is an agent of a foreign power
      1. No U.S. person can be considered an agent of a foreign power based solely on 1st amendment activities (protesting, etc…)
   2. Emergency Provision: When the AG states an emergency situation exists as to foreign intelligence information, warrantless searches are authorized even prior to the FISC acting on the warrant application
      1. Under such emergency, government must submit a warrant application to the FISC within 72 hours of the warrantless search for approval
8. Use of Info Obtained Through FISA Orders: ***United States v. ISA***
   1. Under the 4th amendment, once information is collected, it can be repurposed by government for other uses, this applies to FISA as well
      1. Information properly obtained via FISA can be used in criminal trials
   2. Typically with electronic surveillance in connection with criminal prosecution, must receive a warrant under ECPA
      1. Warrants not required bc target of electronic surveillance was a foreign national
      2. Evidence of crime is not covered by FISA minimization procedures
   3. Potential for FISA to circumvent ECPA
      1. No reason to comply with Title I of ECPA’s warrant requirements, if possible to perform surveillance under FISA order (based upon significant purpose of intelligence gathering of foreign agents) and then, if evidence of a crime is uncovered, they could prosecute it
      2. FISA is not subject to an exclusionary rule, unlike Title I of ECPA
9. FISA “Wall” Between Law Enforcement and NSA/Intelligence Gathering
   1. FISA “wall” does not prevent the sharing of information; it prevents criminal prosecutors from becoming involved in the front end of the investigation rather than the back end
      1. With the “wall,” an official not involved in the criminal investigation must review the raw materials gathered by FISA surveillance an only pass on information that might be relevant evidence
      2. Information that is validly obtained pursuant to a FISA court order can then be used in a criminal prosecution
   2. Under Amended PATRIOT Act, Law Enforcement can obtain a warrant from the FISC as long as it is based upon a significant purpose/national security interest
      1. Law enforcement can be a majority purpose, as long as foreign intelligence gather is still a significant purpose
      2. FISA establishes an easier avenues for electronic surveillance, so little reason now to go through the more difficult evidentiary avenue of ECPA Title 1
   3. Today, there is no real legal “wall” separating information you collect for one purpose and sharing it for another purpose
      1. No constitutional impediment for sharing information regardless of the method it used to collect it
      2. 4th amendment does not deal with data sharing, only data collection
      3. Nexus between criminal activity and warrant can be much weaker under FISA

III. Attorney General’s FBI Guidelines

1. FBI Conduct when Performing Public Surveillance (1976 – AG Levy)
   1. Surveillance could begin when facts or circumstances reasonably indicate that a federal crime has, is, or will be committed (thus opening up an investigation)
   2. Focus on Freedom of Speech and Press
      1. No investigations based solely on unpopular speech, w/ no threat of violence
      2. Techniques designed to disrupt organization engaged in 1st amendment activity, or to discredit individuals would not be used in any circumstance
2. FBI Guidelines did not have the force of law
   1. Provided only a strong sense of comfort to civil libertarians
   2. Forms legal basis to take qualms to courts bc FBI must follow their own guidelines
3. AG Ashcroft Revised the Guidelines in response to 9/11
   1. Eliminated the need for a full case file before FBI conducted certain kinds of surveillance
   2. Cannot tap a phone or apply for a warrant until a full investigation is opened, but can serah out information from other sources (other agencies, public sources)
   3. Allows agents to carry out general topical research, conducting sources every day citizens have access to, before having to open a file (google, etc…)

IV. Homeland Security Act

1. Consolidated 22 federal agencies into the Dep’t of Homeland Security (such as transportation, immigration, secret service, customs and border, etc…)
   1. Does not include the CIA or FBI (political compromise to bring some, not all together)
2. First federal law to create a cabinet agency privacy office, so by law the DHS must have a offer and reports jointly to the head of the agency and to congress
   1. First federal law where an agency senior official must report to the agency head, and then prepare a report for congress (popular model)

V. Intelligence Reform and Terrorism Prevention Act

1. Required executive branch agencies and federal departments to establish an environment to facilitate sharing of terrorism information
   1. Seeks to establish protection of privacy and civil liberties by a five-member Privacy and Civil Liberties Oversight Board
2. Congress shut down the President’s PCLOB and established its own PCLOB as an independent agency located within the executive branch
   1. Has independent authority to oversee confidential privacy issues in intelligence, law enforcement and defense departments
   2. Where others would have no idea (due to confidentiality issues), the PCLOB could investigate these agencies and information to ensure privacy and civil liberties rights
3. As an independent agency as re-established by Congress, no more than 3 members of the same party can be appointed and Senate is to confirm all the appointments
   1. However, it is currently empty as Obama has not appointed anyone

VI. NSA Surveillance Program

1. Terrorist Surveillance Program (General NSA Surveillance Program)
   1. After 9/11, President Bush authorized the NSA to conduct a warrantless communications surveillance program
      1. Kept doing this under AG authority renewed every 45 days
      2. Not clear if it is subject to FISA guidelines
   2. NY Times first revealed (2005) that the NSA was intercepting communications where one party was located outside the US and another party was within the US
2. Protect America Act
   1. Enacted by Congress in 2007 to authorize the NSA surveillance program
   2. Sought a “basket warrant,” generally for surveillance activity involving multiple targets
3. Domestic Surveillance Program
   1. NSA opened offices in the switching rooms of Verizon and ATT, installing large computers, gaining access to the number dialed, length of call, and other information about every domestic phone call made in the US
      1. Information provides link analysis: who knows who
      2. Community of interest subpoena: Records of known targets and everything and everyone he communicates with and who communicates with him
   2. Congress grants immunity (thru state secret doctrine) to phone companies and that ends all civil cases against the non-government targets (Verizon and ATT)
4. State Secret Doctrine
   1. If any party cannot maintain its action or defense without revealing state secrets, then either the entire case must be dismissed, or that claim must be removed (*US v. Reynolds*)
   2. Common law privilege, and it is not formally expressed in any formal statute
5. State Secret Doctrine and No Standing: ***Al-Haramain Islamic Foundation v. Bush***
   1. Court agreed that a sealed document, which the Treasury Dep’t had inadvertently given the Foundation, was protected by the state secret doctrine and not allowed in court
      1. Foundation had been targeted under TSP, as their board of directors was located abroad and they believed it was a terrorist funding organization (w/ Al Qaeda)
   2. State secrets privilege prevented the Foundation (plaintiffs), from reconstructing the essence of the document through memory, denying *in camera* affidavits as well
      1. Without reference to the sealed document, the foundation could not establish that it suffered injury-in-fact; lacking standing
   3. Even individuals who know their privacy was invaded illegally, will not have a remedy when the government has a good case for state secrets
6. State Secrets and Standing Established: ***Hepting v. AT&T***
   1. Plaintiffs alleged that AT&T was collaborating with the NSA in massive warrantless surveillance, namely, the TSP
   2. As customers of AT&T, plaintiffs alleged that they suffered injury from this surveillance
      1. In *Al-Haramain*, court found that the plaintiffs could not show standing due to no access to the sealed document or their memories of it under the SSD
      2. Conversely, *Hepting* P’s alleged injury due to *non-targeted* surveillance under TSP
   3. *Hepting* court found that the existence of the TSP was itself not a state secret
      1. Bush administration had disclosed the general contours of the TSP, which
      2. Requires te assistance of a telecommunications provider, and
      3. AT&T helps the government in classified matters when asked
7. Additional Forms of Authority Gov. uses to Collect Data under National Security
   1. Title 215 of the PATRIOT Act
      1. Allows director of FBI or his designee, to require protection of any tangible thing for an investigation to protect against international terrorism (books, records, etc..)
      2. These tangible things can never be disclosed, and the secrets enclosed in these items die with the recipients of them
      3. Last used in 2006, 47 were issued total
   2. National Security Letters
      1. Relevant to telephone companies, financial industries, ISP, & credit bureaus
         1. Only these industries are subject to NSLs
         2. No court approval needed to distribute NSLs
      2. Records sought are relevant to international terrorism investigation and not conducted solely on the basis of protected 1st amendment rights; kept secret
         1. Issue for communities of interest: not only for a specific person, but for everyone who talked to this person, and people who talked to those contacts
   3. Exigent Letter
      1. FBI issued these exigent letters where they needed data immediately, and attempted to skip over the entire process; illegal to distribute and illegal to comply with

***G. Privacy and Government Records and Databases***

I. Public Access to Government Records

1. Court Records as Public Records: *Doe v. Shakur*
   1. As a practical matter, no access to government documents except for court records, where there is a constitutional right of access
      1. Victim of sexual assault wants to proceed in the civil claim as an anonymous party, in fear of her privacy
   2. Court holds that a woman who is bringing a civil suit (that she was sexually assaulted) cannot bring that suit w/o using her real name
      1. By bringing the suit (and not defending), fairness requires that she should stand by her charges publically
      2. Different situation if this was a criminal suit where state would be prosecuting the defendants, but cannot bring suit independently for money without going public
   3. Balancing notions of fairness, defendants would be at a disadvantage if they were publically accused and open to press scrutiny, and plaintiff’s worked under anonymity
      1. Reinforces the historical openness of the judicial process

II. Freedom of Information Act (FOIA)

1. FOIA Requirements
   1. Right to Access: FOIA grants all persons the right to inspect and copy records and documents maintained by any federal agency, corporation, or department
      1. Facilitates access; where questions arise, preferences should be for access
      2. Does not apply to courts, congress, and certain federal agencies
   2. Requires only that agencies respond to FOIA requests
      1. Congress, President and his advisors, and the NSC are not a federal agencies and not subject to the FOIA
   3. Nine (9) Exemptions to disclosure under 552(b)
      1. National defense or foreign policy
      2. Internal personnel rules and practices of an agency
      3. Specifically exempted from disclosure by statute (other than 552b)
      4. Trade Secrets and privileged or confidential Commercial or Financial information
      5. Interagency memoranda not available to parties
      6. Personnel and Medical files
      7. Records compiled for law enforcement purposes
      8. Regulation or Supervision of financial institutions
      9. Geological and geophysical information and data
   4. Redaction Requirement:
      1. If material can be edited (for sensitive material that would traverse one of the exempt), then the remainder of the document must be provided to the requester
2. Privacy Exemptions (Applies only to Government Agencies)
   1. Personnel and Medical File Exemption (#6)
      1. Files and disclosures that would constitute a **clearly unwarranted** invasion of personal privacy; narrower standard
      2. Only includes files such a medical, personnel, or something clear & unwarranted
   2. Law Enforcement Exemption (#7)
      1. Records or information which could **reasonably be expected** to constitute an unwarranted invasion of personal privacy
      2. Greater range of material falls within this exemption
3. Unwarranted Invasion of Privacy under FOIA: *DOJ v. Reporters Committee* 
   1. Here, SCOTUS recognizes a privacy interest in the rap sheets despite the fact that they are compile from disparate public records
      1. To discover whether an invasion of privacy is unwarranted, government bears burden as to why it should withhold data
      2. Not a 4th amendment issue, focuses on FOIA “unwarranted invasion of privacy”
      3. Generally, once information is exposed to the public, no longer considered private
   2. Central Purpose Test
      1. *EPA v. Mink* established a broad right of access to official info under FOIA, and **invasion to privacy is warranted to the extent it shows what the government is doing, and unwarranted to the extent that it is** **not**
         1. Rap sheet is unwarranted FOIA request to the extent it does not shed light into what the government is doing
      2. Counter to congress, not supposed to ask what the FOIA request is for, but establishes “unwarranted” and does not define it
   3. Bright Line Rule
      1. 3rd party request for law enforcement records or info about a private citizen can reasonably be expected to **invade that citizen’s privacy** when the request **seeks no official info about a government agency**, but merely seeks records the government is storing, the invasion of privacy is unwarranted
      2. SCOTUS basically legislates that all criminal records closed to FOIA unless party seeking info can persuade an agency or court that the collection is to uncover government actions
4. Discretion to Withhold Information: *AFA v. Rose*
   1. AFA compiles records on cases at the academy and redacts the names of people involved
      1. Rose sought records, but AFA declined (even though they were redacted)
      2. Could not be disclosed due to number of facts involved in the cases, where people could figure out who was possibly involved – exempted under the FOIA (vi)
   2. Exemptions grant a discretion to withhold (permissive), but no obligation to withhold
      1. FOIA itself has compulsory language requiring disclosure
      2. Individuals to whom the information pertains has no right to litigate the issue if the agency does not choose to withhold, nor does the individual have a right to be given notice that her personal information falls within a FOIA request
         1. No right to privacy after disclosing information to 3rd party
5. Scope of Exemption 6 – Personnel and Medical Files: *US Dept. of State v. Washington Post*
   1. Exemption 6 is not limited to a narrow class of files containing only a discrete kind of personal information
      1. **Exemption was meant** **to** **cover detailed government records on an individual which can be identified as applying to that individual**
   2. Newspaper seeks passports of detained Iranian national, however denied because those records are very similar to a personnel file or medical record
6. Scope of Exemption 7 – Law enforcement purposes: *National Archives v. Favish*
   1. Favish wants access to crime scene photos of an apparent suicide to perform his own forensic analysis; considered law enforcement records under 7c
      1. Government only needs to prove a reasonably unwarranted invasion of privacy to establish its exemption
   2. Historically, no interest of privacy in the deceased, but court holds that FOIA recognizes surviving family member rights to privacy with their close relative’s death scene images
      1. Family members have a personal stake, and unwarranted public exploitation by intruding on their grief concerning a deceased relative, intrudes on their privacy
   3. Where privacy interest exists under 7(c) and the public interest asserted is to show that officials acted improperly in their duties, requester must establish more than bare suspicion to obtain a FOIA disclosure
      1. Requester must produce evidence that would warrant a belief by a reasonable person that the government impropriety may have occurred
      2. But previously, said that you did not need a purpose for a FOIA request
7. Tenth exemption added to the FOIA
   1. Private sector entities can tell the government about an infrastructure problem and the government must exempt them from the FOIA requests
   2. Meant to increase self-reporting for homeland security vulnerabilities

III. Constitutional Requirements of Public Access

1. Common Law Right to Access Public Records
   1. Under common law, there is a general right to access public records and court records
      1. Right to access is not absolute
   2. Access to public records is justified by desire to keep a watchful eye on gov. operation
2. Court Records
   1. Courts have a long tradition of allowing open access to court records
   2. Every court has supervisory power over its own records, and access has been denied where files might have been used for improper purposes; left to discretion of courts
   3. Pre-trial depositions and interrogatories are not public components of a civil trial, not open to public at common law, and in general are conducted as private
3. 1st Amendment Right to Access
   1. Constitution requires public access to criminal trials
      1. The government can deny access only if the denial is necessitated by a compelling governmental interest and is narrowly tailored to serve that interest
   2. Right to access extends to voir dire in a capital murder trial
4. Privacy of Litigants and Jurors
   1. A court can permit plaintiffs to proceed under a pseudonym, although it is the exceptional case in which a plaintiff may proceed under a fictitious name
      1. Courts can also provide for jurors to remain anonymous
5. 1st Amendment Rights and Right to Privacy: *LAPD v. United Reporting*
   1. SCOTUS aggress that a State can decide not to give out arrestee information at all without violating the 1st amendment
      1. Case was nothing more than a governmental denial of access to information in its possession.
      2. Statute merely required that to obtain arrestees' addresses, respondent had to qualify under the statute; respondent did not attempt to qualify & was denied access
   2. There exists a constitutional right to access in judicial system, no right to access of any other data
      1. California could decide not to give out arrestee information at all without violating the First Amendment
      2. Facial challenge was not warranted because there was no possibility that protected speech would be muted

***H. Government Records of Personal Information***

I. Fair Information Practices

1. In the 1960’s emergence of mainframe computers led to significant debate about privacy
   1. Increased opposition to amount of personal info collected by government agencies
   2. Dept. of Housing, Education, and Welfare issued a highly influential report
2. HEW Report recommended that a Code of Fair Information Practices be established to remedy growing concern over accumulation and use of personal information (5 main principles)
   1. No personal-data record-keeping systems whose very existence is secret
   2. Way for an individual to find out what info about him is in a record and how it is used
   3. Way for an individual to prevent info about him obtained for one purpose from being used or made available for other purposes without his consent
   4. Way for an individual to correct or amend a record of identifiable info about him
   5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data
3. HEW Report’s fair information practices and Watergate inspired Congress to enact the Privacy Act of 1974 after Nixon resigned

II. The Privacy Act (5 USC 552)

1. Purposes of the Privacy Act
   1. Permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by federal agencies
   2. Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose w/o his consent
   3. Allow an individual to access and correct his personal data maintained by federal agencies
      1. Upon request, individuals can review and ask that agency to fix any inaccuracies
   4. Ensure that information is current and accurate for its intended use and that adequate safeguards are provided to prevent misuse of such information
2. Applicability and Scope
   1. Puts in place federal law affecting federal agencies and creates a privacy study commission
      1. Continues in force today with very few amendments
      2. Example of a forward looking act that has been eroded through technology, court decisions, and intentions to circumvent it; little effect on behavior
   2. Applies to federal agencies, not business or private sector organizations
      1. Does not apply to state and local agencies – only federal agencies
      2. Does not apply to all gov info; must be a record maintained in a system of records
   3. PFC of Privacy Act Violation
      1. Agency violated obligations under the act (generally, improper disclosure of info)
         1. Federal “agency” includes any executive department or other establishment in the executive branch of the government (statute says this includes president, cts. say it does not), or any independent regulatory agency (FBI, DOD, etc...)
      2. Information disclosed must be a records contained within a system of records
         1. **Record**: Identifiable to an individual (containing name or other identifying info) and must contain info about the individual
            1. Large data sets like lexis are usually not covered by the PA because they are not structured according to individual identifier
         2. **System of records**: Group of any records under the control of any agency from which info is retrieved by the name of the individual or by some identifying number or other identifying particular assigned to the individual
      3. To collect damages, P must show that an adverse impact resulted from the agency disclosure of PA info and that the violation was willful or intentional
         1. Difficult to distinguish from negligence, thus difficult to prove willfulness
         2. Essentially, must show violation is so negligent, must be willful
   4. **Enforcement**: If an agency fails to comply with any provision of the Privacy Act, or refuses to comply with a request to obtain access or correct individual records, can bring civil action in federal court; in limited circumstances monetary damages may be awarded
3. Limits on Disclosure
   1. No federal agency shall disclose any record which is contained in a system of records by any means of communication to any person or to another agency, except by written request, or with prior written consent of the individual to whom the record pertains
4. Restrictions & Responsibilities for Agencies Maintaining records about individuals
   1. Maintain only the info about a person that is relevant and necessary to accomplish a purpose the agency required to be accomplished by statute or executive order
   2. Collect info to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about that individual rights, benefits and privileges under federal programs
   3. Inform individuals, who make a request, about how their personal info will be used
   4. Publish in the Federal register notices about the systems of records they maintain
      1. This provision allows certain agencies to exempt themselves from requirements of the PA, particularly accuracy and redress/remedies
      2. Generally limited to national security and law enforcement
   5. Publish system of records notice when starting a new system of records
   6. Establish appropriate administrative, technical and physical safeguards to insure security and confidentiality of records
5. Exceptions
   1. **Routine Use**: Broadest exception under the PA; info may be disclosed for any routine use if disclosure is compatible with the purpose for which the agency collected the info
      1. Use that is necessary or proper within the legit scope of the agency to use that info
   2. FOIA: When FOIA requires info be released, PA does not apply
   3. **Info Sharing Among Agencies**: Permits one agency to disclose info to another agency if the agency head makes a written request to the agency which maintains the record
   4. Other Exceptions: Law enforcement, health or safety
6. Information in the Public Domain: *Quinn v. Stone* 
   1. Even publically accessible information is protected against disclosure by the PA because holding otherwise would eviscerate the Act’s central prohibition against disclosure
      1. Information in the public domain is still protected
   2. PA is **not violated** where the agency makes available information which is **already known by the participant**
7. Damages under the Privacy Act: *Doe v. Chao* 
   1. EE’s social security numbers were wrongly disclosed
      1. Did not suffer identity theft, and everyone who said they were not even worried were automatically dismissed; Only Doe said he was worried and made it to court
   2. PA provides for liability in the sum of actual damages as the result of a violation (of one of the 4 PA purposes), but all PA victims entitled to recover at minimum $1000
      1. Doe’s Interpretation: Any P adversely affected by an intentional or willful violation is entitled to the $1,000 minimum on proof of statutory violation
         1. Counter to traditional tort recovery, where proof of harm is needed so damages can be reasonably assessed
      2. Gov’s Interpretation: Minimum guarantee of $1,000 goes only to victims who prove some actual damages (**holding**)
   3. Actual damages is established through some measurable damage
      1. Emotional distress needs to be corroborated by evidence of physical symptoms, medical treatment, loss of income, or impact on behavior
      2. “Concern and worry” or “torn to pieces” is not enough
   4. Court reads the statute as written, and statute expressly provides for liability to victims of intentional or willful violations who sustained actual damages
      1. Only victims w/in a limited class (sustained actual damages) may recover
   5. Dissent’s arguments
      1. Congress sought to afford recovery for any damages resulting from willful or intentional violations of PA (under purpose and legislative history)
      2. Makes no sense to have standing, but not be able to win
   6. Policy: PA is about regulating government activity, ct is getting rid of the penalty for it
      1. Gov’t was not spending to follow law correctly, but used it to fight damages
8. Interaction Between the PA and FOIA: *DOD v. Federal Labor Relations Authority* 
   1. FOIA disclosure supersedes PA non-disclosure
      1. However, if one of FOIA’s privacy exceptions applies, then the PA would require that the government refrain from disclosing certain information
      2. Ex. FOIA exemption for personnel files (exemption 6) is not considered an exception to the PA, it is just a private file, free from disclosure
   2. PA prohibits disclosure unless it must be disclosed under FOIA; FOIA establishes free disclosure of information unless there is an exemption
9. Accuracy of National Crime Information Center Database
   1. DOJ said that the FBI would no longer be required to ensure the accuracy of its NCIC database (which holds 40 million criminal records)
10. Government Access to Private Sector Databases
    1. PA also applies to private companies that contract with the government to administer system of records (essentially all security databases)
    2. PA applies to databases created on behalf of the gov’t, but if the gov’t accesses data from a private database, then the PA does not apply
11. First Amendment Restrictions
    1. Agencies shall maintain no record describing how any individual exercises rights guaranteed by the 1st amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless it is an authorized law enforcement activity
12. Scope of 1st Amendment Restriction: *J Roderick MacArthure v. FBI*
    1. FBI collects information as part of an investigation and maintains that information
       1. Plaintiff wants information of his interactions with groups that may be terrorist organizations expunged from his FBI record
    2. PA does not prohibit an agency from maintaining records about an individual's first amendment activities if the information was pertinent to an authorized law enforcement activity **when the agency collected the information**
       1. Requirement of the statute that information be pertinent to a law enforcement activity **does** **not require** it to be a **current** law enforcement activity
       2. Act does not require an agency to expunge records when they are no longer pertinent to a current law enforcement activity
    3. Reasoning for decision favoring FBI:
       1. Forcing FBI to expunge records with no current law enforcement necessity, would place substantive and administrative burdens upon the FBI and other government agencies, with little or no gain to individual privacy (but this is irrelevant)
       2. Information once collected as part of a closed investigation might play a role in a new or reopened investigation
    4. First Amendment Claim & Standing
       1. Need an injury, traceable to the defendant, that is capable of redress
       2. Court says no injury from having personal information stored in an FBI database
       3. Plaintiffs lack standing for a claim of 1st Amendment violation based upon creation of files based upon associational activity due to lack of standing
    5. Dissent resorts to the plain meaning of the statute
       1. Interprets 1st Amendment restriction as requiring that records be pertinent to an authorized LEA not only at time of gathering, but also at time of maintaining
       2. If there is no current law enforcement to which a record has pertinence, the agency may not maintain it (which means to preserve, keep in existence)
13. Recommendation for Amendment **(What report?)**
    1. System of records definition should be eliminated and PA should simply apply to all government records
    2. Because privacy notices have become so bland and all encompassing, recommendation that law be amended to require federal register notices that include detailed purposes

III. Use of Government Databases

1. Computer Matching and Privacy Protection Act
   1. Regulates the practice of computer matching
      1. Generalized electronic search and cross comparisons of millions of records in order to detect fraudulent activity
   2. CMPPA essentially accomplishes nothing – Problems of repurposing data:
      1. Data not accurate for purpose not being used
      2. Matching is difficult due to name changes, middle names
      3. If data is corrected in one database, other one may not be updated
      4. Only positive is that it shows that congress became aware of the danger of free sharing information between databases
   3. Amends the PA and provides that in order for agencies to disclose records to engage in computer matching programs, they must meet 6 requirements:
      1. Written agreement between the source and recipient agency or non-federal agency stating the purpose and legal authority for the program
      2. Legal justification for the program
      3. Description of the records to be matched
      4. Procedures for the accuracy of the information (pretty weak in reality)
      5. Prohibitions on redisclosure of the records
      6. Requirement of a data integrity board within each agency to oversee matching
   4. If computer matching negatively affects an individual, must establish why to receive the right to appeal
2. Airline Passenger Screening: 9/11 Commission Report
   1. Under CAPPS (computer assisted passenger prescreening system), air carriers enforce government orders to stop certain known and suspected terrorists from boarding commercial flights and to apply secondary screening procedure to others
      1. CAPPS was the initial form of passenger screening, and used behavioral data of activity with airline (one way tickets, etc…), did not use info about individuals
      2. Concern over sharing intelligence with private firms and foreign countries keep the US government from listing all terrorist suspects who should be included
   2. Proposed that screening be performed by the TSA and should utilize larger sets of watch lists maintained by the federal government
3. Evolution of Passenger Screening
   1. CAPPS II:
      1. Classified people according to color coded threat level
      2. Problems with large number of false positives; abandoned quickly
      3. This analysis requires sensitive data that was undisclosed, and inaccurate
      4. Terrorists could just pick someone not matching the target group
   2. Secure Flight
      1. Computerized, minimalistic system that narrows number of people whore are intrusively searched
      2. After providing name, birth date, gender, checks to see if you match a name on a no-fly list
4. Government Data Mining
   1. Data mining involves examining personal information in databases to look for patterns or unusual activity, or to identify links between a suspect and other individuals
      1. Deals with how we analyze data
      2. Ex. Computer matching programs is data mining – they seek to detect fraud by making comparisons in personal info residing in different databases
   2. Total Information Awareness (TIA)
      1. DOD project that would consist of a database of dossiers of people with info about their finances, education, travel, health, and more
      2. Information would be obtained from numerous private sector company and used to profile people to single out those engaged in terrorist activity
         1. Reasoning: More data lists = catching more terrorists
         2. In reality, it was a tool that different agencies could use for their own purposes; poorly handled and was shut down by congress
      3. “Red Teaming” – intelligence officers would simulate terrorist behavior, evaluate data trails they created, and perform pattern analysis with database
         1. “Red teaming” is supposed to imagine new attacks, however this process would be based off past events and evaluating the wrong things
         2. Patterns of terrorist activity resemble patterns of normal life for too many people (students, low income, etc…); would signal too many people
   3. 4 types of data mining (pattern and subject based are at opposite ends, other 2 in-between)
      1. Subject based: Attempt to get info on a specific, individual subject; justified by some suspicion
      2. Pattern based: Search for anyone who has done a set of actions in common that we think is suspicious; unsure if crime has been or is being contemplated, just want to know who fits this criteria
      3. Relational or link based: Start with something or someone and look to see who is related, continuing to follow the links (relationship among people, data, or things)
      4. Data matching based: Want to see what two data sets have in common
         1. Airline watch lists compare to passenger lists; tax auditing
5. Technology and Privacy Advisory Committee (TAPAC) Report
   1. TAPAC examined privacy implications of data mining
      1. TIA was a flawed effort to achieve worthwhile ends
      2. Flawed by perceived insensitivity to critical privacy issues, the manner in which it was presented to the public, and lack of clarity and consistency which it was described
   2. Central recommendation is for a FISA court to approve various data mining projects
      1. Where data mining involves personally identifiable info about US citizens based on no particularized suspicion need to establish need for data mining to prevent/respond to terrorism, and obtain authorization from FISC
      2. If there is particularized suspicion about a specific individual, existing law should govern; allows searches seeking to identify or located suspected terrorists
6. Reasonable Suspicion and Criteria Profiling: *US v. Sokolow* 
   1. Police can stop and briefly detain a person for investigative purposes if the officer has a reasonable suspicion supported by articulable facts that criminal activity may be afoot
      1. Officer is not required to have probable cause, but must be more than a hunch
      2. 4th Amendment requires some minimal level of objective justification for the stop
      3. Stop must be considered under the totality of the circumstances
   2. The profiling of Sokolow’s acts and behavior (after a subject based data mine) and agent’s belief that it was consistent with one of the DEA’s drug courier files, taken altogether amounted to reasonable suspicion sufficient for a Terry Stop
      1. Ticket agent was suspicious of Sokolow and informed a local officer who later determined phone numbers, aliases, and scheduled stopovers
         1. Drug sniffing dog named **Donker** eventually found cocaine in their bag
      2. Paying for tickets in cash, not checking any luggage, destination was a drug haven, reasonable belief that Sokolow was under an alias, and the brevity of the trip, **taken together could establish reasonable suspicion**
         1. Though each act may not singularly be probative of any criminal activity
   3. When determining reasonable suspicion, agent must articulate factors that led to his individualized suspicion, and the fact that these factors may be set forth in a “profile” does not detract from their evidentiary significance as seen by a trained agent
7. Data Mining of Inaccurate Information: *Arizona v. Evans*
   1. Exclusionary rule does **not** apply to evidence seized in violation of the 4th amendment by an officer who acted in reliance on a police record that is later determined to be erroneous
      1. After pulling over Evans, he notified the officer that his license had been suspended who proceeds with a data mine in a computer data terminal which indicates the erroneous outstanding warrant
      2. This led to his arrest and search of the car which uncovered marijuana, which Evans seeks to exclude here as an illegal search and seizure
   2. Because court EE’s were responsible for the erroneous computer record, exclusion of evidence at trial would not sufficiently deter future errors so as to warrant the use of the exclusionary rule
      1. No indication that officer was not acting objectively reasonably when he relied on the police computer record
      2. Exclusionary rule was historically designed as means of deterring police misconduct, and supports a categorical exception to the exclusionary rule for clerical errors of court EEs (no deterrent effect on them even if applied)
   3. Dissent argues that mistakes by databases like the NCIC can infect nation wide information, and in the electronic age, with respect to record keeping, court personnel and police are not compartmentalized
      1. Artificial to distinguish between court clerk and police slips bc it may be difficult to pinpoint who actually caused the error
   4. This case establishes that there is little legal incentive to have accurate records if you are the police, there are practical incentives, however, there is no punishment for government maintaining outdated records
      1. Data mines subsequently could turn up false positives and wrongful arrests with no repercussions
8. Data Mining under the 4th Amendment: *US v. Ellison*
   1. Officer notices an illegally parked van (but does not issue a citation or request them to move), and when the van moves into a legal spot the officer runs the license plate number in his Law Enforcement Information Network
      1. Revealed outstanding felony warrant, and when he confronted him and patted him down found firearms, and charged him with a felony
   2. Individuals have no right to privacy in what they knowingly expose to the public
      1. Ellison had no privacy interest in the information (license plate number) retrieved by law enforcement
      2. Technology used in this case does not allow officers to access any previously unobtainable information, rather allows them to access more quickly
      3. Information was obtained without intruding upon a constitutionally protected area, and no search for 4th amendment purposes
   3. Because individual had no reasonable expectation of privacy in the information contained on his license plate (which he knowingly exposed to the public), there is no probable cause required to run a data mine based on that knowingly, publically exposed information
      1. Essentially did not need particularized suspicion to engage in an investigation of someone without sanction

IV. Driver’s Privacy Protection Act

1. DPPA is a federal mandate restricting State DMVs from selling personal information (motor vehicle records) about any individual to any commercial entity
   1. Personal Information – data that identifies an individual (SSN, photo, name, etc…), and specifically excludes info on accidents, driving violations and driver status
   2. Applies to state DMVs and their officials and employees, and only motor vehicle records
2. Controversial bc federal government tells state governments what to do
   1. Congress did not apply ban to federal databases, only to the states
      1. States could no longer sell records to other for marketing purposes
   2. Commerce clause says congress can regulate interstate commerce, and data is an item in commerce, and control of sale of vehicle data is sufficient under federal legislation
3. Exceptions
   1. Personal info can be disclosed for purposes of law enforcement, recalls, legal proceedings, and insurance claims investigations
   2. Permits disclosure to licensed private investigation agencies
      1. Ironically, event that motivated DPPA was murder of Rebecca Shaeffer after murdered got her address from a PI who got it from the DMV
   3. Journalists were significant users of vehicle records, and when court decided **against** a 1st amendment public interest use exception, PI’s still had access, but journalists did not

III. PRIVACY AND THE PRIVATE SECTOR

***A. The Financial Services Industry and Personal Data***

I. The Fair Credit Reporting Act

1. Growth of National Credit Reporting
   1. The past was based on captive reporting (where Sears and other retailers had their individual or regional information bureaus)
   2. Today, there are 3 national credit bureaus that maintain credit reports on anyone over the age of 18; no reports on children are allowed
      1. National Credit Bureaus: (1) Experian; (2) TransUnion; (3) Equifax
   3. Credit report data is based on transaction data, not granular data
      1. Does not focus on individual transactions, rather information that follows credit cards, mortgages, and loans
         1. Average American has 12 credit lines (usually credit cards)
         2. Single delinquent payment can affect your credit
      2. Credit issuers, amount of credit available, history of delinquent payments
2. Introduction to the FCRA
   1. Concerns about the FCRA
      1. Accuracy; whether data in the credit reports are accurate, how can you be sure
      2. Privacy; to what extent is privacy infringed in use or collection of the data
      3. Fairness; lack of accuracy or privacy can make reports inherently unfair
   2. FCRA is first privacy act that focuses on use of data, rather than restricting collection
      1. Establishes a structure that permits the collection of data entirely, without much regulation bc it focuses on use of data instead
      2. Creates a regulated class of Consumer Reporting Agencies (CRAs or credit bureaus) – defined broadly to include anyone who collects and furnishes data about other consumers (consumer reports used in employment, insurance, and credit)
3. Scope of the FCRA
   1. FCRA applies to any consumer reporting agency that furnishes a consumer report
      1. Creates highly regulated class of consumer reporting agencies, with little regulation of users and furnishers of data
      2. Main focus is on credit bureaus, legal compliance focuses on these agencies
   2. Consumer Reporting Agencies (CRA):
      1. Any person, which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in assembling or evaluation consumer credit information or other information on consumers for the purpose of furnishing consumer reports to 3rd parties
         1. Must furnish consumer reports;
         2. Must be in the business of doing so; and
         3. Must be evaluating individuals, not businesses
      2. Consumer information must be supplied by a third party; if reporting only what you gathered through first hand experience with a consumer, you are not a CRA
         1. Not a CRA if you report specific extension of credit
         2. Ex. 3rd party company notifies you that you have failed to pay credit card
   3. Consumer report (3 requirements)
      1. Written or oral communication of any information of a consumer by a consumer reporting agency
      2. Information must bear on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living
      3. Information must be used or expected t be used as a factor in establishing a consumers eligibility for credit or insurance, establishing a consumers eligibility for credit or insurance, employment, or any other authorized purpose under 1681(b)
4. Ten (10) permissible purposes where a CRA can provide a consumer report
   1. Court order or grand jury subpoena
   2. To the person to whom the report pertains w/ written consent
   3. To a person which [the agency] has reason to believe will use the information for
      1. Extension of credit to a consumer, review of an account
      2. Employment purposes
      3. Insurance underwriting involving the consumer
      4. License or the conferral of government benefits
      5. Assessment of credit risk associated w/ existing credit obligation
         1. Ongoing credit obligations allows creditor to view the account
      6. Determining eligibility for a license or other government instrumentality required by law to review financial responsibility (treasurers, secret agents)
      7. Legitimate business need for a business transaction involving the consumer
         1. If consumer initiates a transaction (applying for credit card, home loan)
         2. If account already exists, can look to see if you continue to meet requirements of the account
   4. To establish a person’s capacity to pay child support
      1. Agency administering the child support can receive records to see who should be paying, and how much
5. Exceptions to Permissible Purpose Requirement (Still must be based on a single, initial PP)
   1. Sharing of transaction and experience information **among affiliates**
      1. Reporting your own experiences with a consumer to a third party is not a credit report, only when a third party reports that information does a credit report exist
      2. Exception extends to all affiliate of a conglomerate, where affiliates can report transaction experiences with an individual consumer to all the other affiliates without becoming a CRA
      3. Practically, where a pre-existing conglomerate with several affiliates (Citibank has 4,000) purchases another affiliate, it would be grandfathered into the exception
   2. An agency can share a 3rd party prepared credit report with other affiliates if:
      1. The initial agency had a legitimate purpose for receiving the initial consumer report
      2. The consumer is given an opportunity to object/opt out
      3. Only one permissible purpose is need among all affiliates before the information from the consumer report can be shared (fiscal reasons, why buy it 4,000 times?)
   3. Joint-User System
      1. If 2 or more companies are involved in the same transaction, if one of the companies receives a consumer report, it can be shared w/ the other companies
6. Certain circumstances require consumer consent even if a permissible purpose exists
   1. Explicit consent is needed for medical information; federal law requires consent if disclosing a known condition (e.g., cancer)
7. Unauthorized Disclosures of Credit Reports: Prescreening
   1. Common practice where a company seeks a list of consumers from a CRA who meet certain criteria in order to market from them
      1. Not an express permissible purpose
   2. CRA can provide a credit report, without the consumer’s authorization only if:
      1. Transaction involves a firm offer of credit or insurance (everyone who meets the prescreen criteria receives an offer);
      2. At the time you are contacted, company must give you the opportunity to opt out of the pre-screening (2 years by phone, letter is permanent opt out)
8. Requirements for Consumer Report Accuracy
   1. Agency must follow reasonable procedures for maximum possible accuracy
      1. Reasonableness; there is no liability for inaccurate data, unless it arises out of unreasonable procedure
      2. Only need to achieve max level of accuracy possible; CRAs not required to achieve impossible accuracy standards
   2. Consumer must be given notice and opportunity to detect error, and the CRA must have vigorous dispute resolution process
      1. Remedial accuracy is the key; time limits set for days of investigation (30 days)
         1. Preventative accuracy is too expensive, that is why remedial is the approach
      2. Because three agencies are on different cycles, depending on the dates you receive a credit report data could be different (typical mistake is data placed in wrong file)
      3. Burden is on consumer to determine accuracy of your report
   3. Limits on obsolete information
      1. Data in consumer report is limited to 7 or 10 years, ability to outgrow mistakes
         1. Default on credit card at age 19 not furnished by CRAs at age 26
      2. Data stays in the file forever, there is no limit to collection of data, only a limit to the furnishing of data
         1. If certain requirements are met, obsolete info can be used in a report
         2. Nothing is deleted unless erroneous, just not furnished
9. Modest Requirements for Regular Furnishing of Information
   1. Obligation to use reasonable procedures for accuracy and to correct errors
   2. Regulation is for large companies like Citibank or Bank of America who furnish enormous amounts of information on a regular basis
10. Identity Theft: Fair and Accurate Credit Transaction Act (FACTA)
    1. CRA and furnishers shall block the re-reporting of any information in the file of a consumer that is the victim of identity theft
    2. Even if the FTC sees something in the file that needs to be adjusted, not allowed to
11. *Smith v. Bob Smith Chevorlet* 
    1. Auto dealership must have a reasonable belief that the debt (permissible purpose) existed to access the credit report; must have legitimate business purpose behind the credit report
    2. Only alleging the existence of a permissible purpose is not enough, here credit report was not based on reasonable belief that debt was owed, was based on a belief of a mistake
12. *Sarver v. Experian* 
    1. Experian erroneously informed others through credit reports that Sarver was bankrupt
       1. No liability for inaccurate information, only for unreasonable processes
       2. Finding of liability also requires that consumer suffered harm (Sarver was turned down for credit, arguably because of erroneous credit report)
    2. Only receive compensation for errors **after** a dispute is established with the CRA
       1. Sarver did not dispute the report before hand, only disputed it after he was turned down for credit, which prompted him to ask for credit report, which is when he saw the error (no dispute before harm occurred)
          1. Failure to correct did not harm him in this situation (timing)
       2. Had Sarver originally received his report, requested the change for inaccuracy, and Experian then did not fix it and he was turned down for credit, winning claim
    3. No evidence of willfulness or unreasonable procedure to effect max accuracy possible to establish a separate claim for violation of the FCRA
13. *Dennis v. BEH-1, LLC*
    1. Settlement discharges a lawsuit, and defendant is presumed innocent and discharged with prejudice; however, Experian puts in his credit report that there was judgment against him
       1. Consumer contacts Experian of the mistake, and Experian then sends the complaint to a 3rd party contractor who screws up and says that Experian was right
    2. Consumer argues that Experian failed to maintain reasonable procedure to ensure accuracy of credit reports and it failed to adequately reinvestigate the disputed information
       1. Even though Experian is consistently wrong, it has still complied with act
       2. Experian does not have to be correct, only compliant with the FCRA

II. Gramm-Leach-Biley (GLB) Act

1. Use and Disclosure of Financial Information before the GLB Act
   1. Glass-Steagall act was passed in response to the depression to prevent different types of financial institutions from affiliating with each other
      1. This broke up huge financial conglomerates, but was pressure to overturn this act
   2. GLB act reverses the GS act, and enables the creation of financial conglomerates that provide several different forms of financial services
      1. Allowed companies that were legally separate to combine their operations and data
      2. Merge of Citibank and travelers insurance occurred parallel to the GLB act raising concerns of mixing medical and financial information
   3. Congress passes Title 5 of the GLB act in 1999 over increasing privacy issues due to companies having more complete and complex profiles of customers via mergers
2. Introduction to the GLB Act
   1. Authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies
   2. Permits sharing of personal information between companies that are joined together or are affiliated with one another
   3. Can also share information between unaffiliated companies (though consumers can opt out of this sharing; cannot opt of anything else)
3. Who enforces the GLB Act
   1. Any federal agency that regulates financial institutions
   2. State insurance commissioners
   3. FTC; if you provide a financial service but are not regulate, fall under rule of the FTC
4. To what does the GLB Act apply
   1. Applies only to **nonpublic personal information** that consists of personally identifiable financial information (required to meet 1 of 3 conditions)
      1. Provided by consumer to financial institution (opening an account and providing your information)
      2. Resulting from a transaction with a consumer (write a check, use your card)
      3. Otherwise obtained by the financial institution (buys a list, etc…)
   2. Nonpublic personal information means personally identifiable financial information, however obtained by the institution (as stated above)
      1. Nonpublic does not appear in the definition
   3. Contrast with Regulation P’s definition of nonpublic personal information
      1. Personally identifiable financial information
      2. Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information
      3. Any information obtained through the three stated ways
5. Privacy Rights under Title 5 of the GLB Act
   1. Detailed (but not very restrictive) privacy rules governing operations of the financial services sector
   2. The act permits financial institutions that are joined together to share the nonpublic personal information that each affiliate possesses
      1. Suppose an affiliate has access to a person’s medical info, that info could be shared with an affiliate bank to turn someone down for a loan
      2. Affiliates must tell customers that they are sharing such information, and can be done through a general disclosure of a privacy policy
      3. No way for individuals to block this sharing of information
   3. Rules effectively required financial services institutions to:
      1. Send each of its customers an annual privacy notice that, at the minimum, describes policy and practices with respect to disclosing nonpublic personal information
      2. Comply with any other disclosures required by state or federal law, provided annually and by writing, unless the relationship is electronic
   4. Requires FTC and other agencies to establish security standards for nonpublic information
      1. Establish information security programs to protect categories of nonpublic personal information that it has and discloses
   5. GLB Act leaves open option for more serious privacy enforcement through state law
      1. Acts as a privacy floor, not a ceiling
      2. Ex. California; adopted rules even more restrictive than the FCRA, but the FCRA (unlike GLB) supersedes other laws, and this law was thus struck down bc it prohibited affiliates from sharing credit information (but FCRA explicitly allows it)
      3. Ex. North Dakota; voters passed further restrictions, constitutional because it did not violate FCRA (allowed affiliate sharing), only denied 3rd party sharing
6. Exceptions to use of nonpublic personal data under the GLB Act
   1. Restrains the ways in which financial institution could use nonpublic personal data, but so many exceptions to the Act essentially made everything an exception
   2. Only thing that **consumer can opt out** of and object to, is the transfer of data to a non-affiliated 3rd party for marketing a nonfinancial good or service
      1. Ex. If chase wanted to refer you to check wiring, credit protection, or other joint marketers it is okay (as long as sharing information to affiliated companies), but if they are selling information to Sears to discover TV purchasers, you can opt out
7. Changes under the GLB Act
   1. Pre-text calling
      1. Generally used by investigators, call banks pretending to be someone you are not
      2. Legal for law enforcement and child support collection agencies to do this, but now illegal for everyone else
   2. No sharing of account numbers
      1. Financial institutions cannot disclose (other than to CRAs) account numbers or credit cards for use in direct marketing (telemarketing, email, mail)
      2. Can share up to 4 numbers for identification purpose, but if individuals want to buy a good or service, must provide full number themselves
      3. Makes it more difficult to engage in fraudulent marketing
   3. Security rules that financial institutions must follow to secure customer data
      1. Financial institutions must use multi-factor authentication w/ their online services
      2. Transactional data, things you memorize, something they sent you, thumb drive…?
8. GLB Act is indicative of most modern privacy law
   1. Provides essentially no privacy protection whatsoever
   2. Very expensive, and trillion notice must be mailed
      1. Each institution has to send all customers an annual notice
      2. Congress described financial institutions very broadly, and essentially anyone that extend financial credit is considered a financial institution (health care, credit, banks, investment, pensions, liability, retirement, etc…)

III. Identity Theft

1. Three (3) different activities considered Identity Theft
   1. Existing account fraud
      1. Fraud of credit cards, checking accounts, and unknown charges
      2. Constitutes 1/2 to 2/3 of all reported frauds of the 10% victims that spent at least 55 hours resolving their problems
   2. True Identity Theft (New Account fraud)
      1. New account is opened by someone else in your name
      2. Constitutes 1/3 to 1/2 of all reported frauds of that 10%
   3. Synthetic Identity Theft
      1. Someone else’s identity is not used, a brand new identity is created
      2. Banks are not required to report this, and tend not to, because they do not want people to know they are extending credit to non-existent people
      3. Remedial accuracy only exists where the person actually exists
      4. Could constitute up to 90% of financial fraud, but cannot be measured as of yet
2. Statistics about Identity Theft/Fraud
   1. US has the lowest fraud rate of any industrialized nation in the world; approximately 2 million people suffered some form of financial fraud last year
      1. Estimations are so much higher because individuals are becoming more and more apparent that it is happening to them
      2. Friends or family members are the most common purveyors of identity theft/fraud
   2. In the vast majority of cases, the effort to defraud is blocked
      1. The maximum an individual can suffer for existing account fraud is $50, and any other amount is usually taken care of by the bank
      2. Cots are eaten by businesses dealing with individuals, individuals are not suffering losses on the whole
      3. Total fraud loss per person (including businesses) is a median loss of $300
      4. Median response for amount lost from a fraud is $0, and 5 hours spent dealing w/ it
3. Identity Theft Assumption and Deterrence Act
   1. It is a crime in the US to commit identity theft and any acts leadings up to it
   2. Impersonations, use of someone else’s credentials, etc… are all illegal
4. Credit Freeze: Way to combat identity theft or fraud
   1. Instruct not to release your credit score to anyone in any effort obtain more credit
   2. No one can establish credit in your name, but you cannot do it either
   3. This does not work with synthetic identity theft, because there is no one to establish the fraud alert on a non-existent personal identity
5. *Sloane v. Equifax*: Identity theft and responsibilities of CRAs
   1. Example of credit bureaus gone wild, where incorrect information is failed to be fixed and is continued to be re-reported
   2. Equifax's continued failure to respond to the plaintiff's requests (21 months after first complaint) and to follow mandated "reasonable" procedure to correct her credit report and remove fraudulent accounts brought significant problems on her family
      1. Failure to fix errors in credit report stemming from identity theft led to denial of credit for home loans and car purchases
      2. Established emotional and economic damages reward for Sloane
   3. What occurred to Sloane no longer happens today, because as of 2008, as a regulated entity, credit bureaus are obligated to keep records of when identity theft occurs

***B. Commercial Entities and Personal Data***

I. Governance by Tort

1. Tort for Invasion of Privacy: *Dwyer v. American Express Co.*
   1. Four elements to claim an intrusion upon seclusion tort
      1. Unauthorized intrusion or prying into the plaintiff’s seclusion;
      2. An intrusion which is offensive or objectionable to a reasonable man;
      3. The matter upon which the intrusion occurs is private; and
      4. The intrusion causes anguish and suffering
   2. Targeted mailing list assembled by the credit card company based on spending patterns, without revealing any specific purchases, just general groupings (value purchasers, etc…)
      1. That info is given to a 3rd party fulfillment house, who sends out these mailing lists to companies that have an interest in them
      2. Nothing is actually given to the company by AMEX, fulfillment house receives it and they are under strict privacy provisions
   3. Claim does not get past first element, because there was no unauthorized intrusion or prying alleged to even establish a cause of action
      1. When signing up for a credit card, voluntarily disclosing information to the defendants that, if analyzed, will show shopping and spending habits
      2. Credit card company was only doing analytics that it was allowed to do, and the product of that analysis are the grouped lists of consumers
   4. This is pile on litigation (suit was brought only after NY AG settled with AMEX, saying they were no longer going to do this under state law)
      1. Pile on litigation fails P cannot establish any demonstrable harm
2. Value of Consumer Names: *Shibley v. Time*
   1. The individual names of consumers only have value when associated with [subscription] lists (that were sold to direct mail advertising business)
      1. The value in these consumer lists is not in the individual names; the value is the association with the criteria the list is based on
   2. There is appropriation of the industry value that AMEX or any other company that preformed the analysis, added to these consumer lists
      1. There is no appropriation of individual name value
      2. Value of these lists are only established by 3rd parties wanting that information
3. Single **Exception** to Tort Approach on Info Privacy: *Remsburg v. Docusearch*
   1. Docusearch provides a client the workplace address of Amy Boyer (which they obtained through an illegal pretext call), and client subsequently goes and kills her
      1. Note that this is not a SCOTUS holding, only New Hampshire state court
   2. Did Docusearch have any duty to Amy Boyer?
      1. Existence of duty arises from need again reasonably foreseeable harm
         1. Duty is typically established through special relationship (doctor, etc…) or the duty is voluntarily assumed
      2. Analysis is muddied because there is no general duty to protect others from the criminal attack of 3rd parties, but this arose out of criminal misconduct
   3. In unusual circumstances, there is a recognized exception to the no general duty of care
      1. If there is a special temptation for criminal misconduct brought about by the misconduct, duty to exercise reasonable care to prevent the risk from occurring
   4. Issue is Foreseeable Endangerment
      1. Court finds that it was foreseeable that information could be used for harm when Docusearch provided that information (stalking, identity theft, etc…)
      2. Threats and risks of criminal misconduct is sufficiently foreseeable, so Docusearch ad duty for reasonable care in disclosing 3rd party personal information to the client, especially because they did not know client’s purpose for seeking the information
4. Cate disagrees with Court’s Analysis in *Remsburg*
   1. Question should not focus on forseeability of harm, rather:
      1. Hw much data that Docusearch provides could be used for stalking;
      2. Whether Docusearch had encountered this situation before
   2. Information about where an individual works in not private, general public knowledge
      1. Decision raises issues of establishing boundaries on any general duty that arises providing information (assuming there is liability in tort), when considering the information services that are readily available
   3. Possibilities for limiting scope of *Remsburg*
      1. Restrict conduct to legally available information (eliminates pretext calling)
      2. Limit by requiring payment for services
5. Tort approach has **failed** miserably for informational privacy
   1. Scott McNealy (CEO) of Sun Microsystems: Individuals have zero privacy, get over it
   2. Tort law is not a good fit for informational privacy, and almost uniformly has not allowed tort law to apply because there is no general duty of care and generally no harm caused

II. Governance by Contract and Promises

1. Contract Law and Informational Privacy
   1. K requires consideration, reliance, and clarity on terms of the deal
      1. Ideally, both parties read it, or relied on it to their detriment
      2. Cannot sue for breach of k if you did not know you had a k
      3. Cannot sue if there is no consideration
   2. Breach of K tends not to work in informational privacy because there are no contracts, generally there are only privacy policies
2. Privacy Policies
   1. Statements made by companies about their practices regarding personal information
      1. Privacy policies are required for financial institutions, insurance companies, and brokerage companies under the GLB Act
      2. No K action under a privacy policy; breach of k claims continue to fail
   2. Opt-out: Establishes a default rule that the company can use or disclose personal information in the ways it desires so long as consumer does not indicate otherwise
      1. Consumer must take affirmative steps to opt out of a particular disclosure
      2. GLB Act is an opt out, and can only opt out of one thing
   3. Opt-in: Establishes a default rule that the company cannot use or disclose personal information without first obtaining the express consent of the individual
3. Issues of Choice in Privacy Policies
   1. Opt-out is the traditional method in US privacy, but US laws are increasingly moving towards opt in policies
   2. Under opt-out, business have incentive to be unclear, whereas under an opt-in, there is huge incentive for business to be clear in order to gain access to information
      1. Either way, consumers never act on the opt-in, or opt-out
   3. Ex. Under an opt-out, MBNA can use info from credit reports to immediately see who qualifies and send out those offers
      1. Under an opt-in, company would have to contact everyone first, ask for permission to search for their credit card eligibility (and there is only 3% response rate)
      2. Alternatively, could offer everyone a credit card due to opt in, and the people who shouldn’t get those cards would get them and probably default
4. Requirements for a Policy Privacy
   1. Four (4) requirements for a policy (+1 unofficial)
      1. Notice: prominent notice of how, why, and what data is collected
      2. Choice: if consumer has any choice and how to exercise it
      3. Access: level of access consistent w/ business uses of data involved
      4. Security: must outline broadly their security practices
      5. FTC requires some enforcement (unofficial prong)
   2. Requirements do little for individual privacy
      1. Privacy policies could only tell consumers that they have no choice or no privacy and still be considered legitimate
      2. Even by only saying that consumers privacy, that is a good policy whether or not that security is actually provided
5. FTC v. Eli Lily: First FTC case for violation of company privacy policy
   1. Alleged failure to provide adequate privacy as promised under the policy, when Eli Lily erroneously sent out an email with the names of all the recipients
      1. None of the 800 people whose names were released read the policy, and there was no harm, but commission said that they violated their privacy policy
   2. Section 5 of the FTC Act (15 USC 45): Legal authority for failure to adhere to policy
      1. Prohibits unfair or deceptive trade practices
         1. Consumer is deceived, company omits a material term or misleads/falsifies a material term
      2. Unfair practices meet there requirements
         1. Cause or potentially cause substantial injury to consumers
         2. Injury is not easily avoidable by consumer
         3. No significant countervailing benefit to consumers or competition
         4. Deception is established when there is a promise that is broken
   3. Case is settled (dominant form of legislation for commerce in the US)
      1. Settlement order lasts 20 years, includes direct oversight by FTC, reports filed to the FTC, audits of privacy practices, and attorneys fees (no punitive fine or admission of wrong doing)
      2. FTC act is primary enforcement tool for privacy policies; policy is not a k, so if it is deceptive commercial practice, actionable under FTC act
6. FTC Act: **Deception** is established when a promise in a policy is not met
   1. Company promised adequate privacy, failed to deliver because it released email addresses of those who signed up on their website
   2. Deception does not required consideration or harm (unlike k law); irrelevant that no one was injured and that no one read the policy
7. FTC Act: **Unfair practices** do **not** require an explicit promise to be actionable
   1. Deception requires a broken promise to be deceptive, where unfair practices do not have to meet any such prerequisite
   2. FTC Act violation exists even if the entity was silent, if a practice is
      1. Likely to cause substantial harm to consumer;
      2. That harm is not outweighed by countervailing benefits; and
      3. That harm was not easily avoidable
   3. Earliest unfairness violations was over security of information
      1. Holding credit card transactions over unsecured online networks led to risk of stolen cc information
      2. Nothing the consumer could do, and there was no benefit gained from these unencrypted cc transactions
   4. Unfair practices violations are much broader bc they do not rely on past promises
      1. Violations generally described or defined after the fact
      2. Unencrypted cc violation was deemed unfair by the FTC 3 years later
   5. Ex. *Sears v. FTC* (settled last summer)
      1. Sears disclosed what it was doing with consumer data in its privacy policy
      2. FTC said policy was unfair because it did not disclose it prominently
      3. First case where, even though entity had full disclosure, policy was still unfair
      4. This is considered the future of FTC enforcement power
8. Example FTC Order: *In the Matter of Vision I Properties* 
   1. Decision and order by the FTC accepting a settlement with a company that engaged in practice where it sold, traded and lended information on customers or visitors
      1. “Broken Promise” case: Entity promised not to do something in its policy and it did it anyways (deceptive policy), and it was in interstate commerce (anything online)
   2. Company does not admit liability
      1. Subjected to 20 years of FTC oversight
      2. Pays $9,000 disgorgement (profits earned by policy violation) and attorneys fees
      3. Promises not to violate policy again in the future
      4. Subjects itself to FTC oversight (send copies of its privacy policy to the FTC) and oversight of the corporate structure
9. Procedure for Changes to a Privacy Policy
   1. FTC prefers that the policy changes are made prospectively, where data already held is under the old policy, and any new data received is regulated under the new policy
      1. Most companies do not go this far; no specific law to require them to do so
      2. Managing this change is difficult bc FTC provides no guidelines to changes, and **change is the only constant in business**
   2. Companies generally find an approach that is economically advantageous, w/ no immediate law suit from the FTC
      1. Depends how big the change to policy is, and how sensitive the information is
   3. Providing consumers the change to opt-out, prominent notice of the change, and opportunity for consumers to ask for their data to be deleted under the new policy, is generally sufficient for a policy change (as long as the information is not very sensitive)
10. Privacy Promises and Bankruptcy: *FTC v. Toysmart* 
    1. Privacy policies may say that the entity will never sell customer data, but in bankruptcy, this consumer information is a viable asset
       1. Bankruptcy court said that the consumer data had to be sold to pay creditors, but FTC tried to stop it because there was sensitive information about children
       2. Walt Disney just bought the information and destroyed it
    2. Bankruptcy code amended to provide that in bankruptcy cases with sensitive information, privacy ombudsmen twill advise court as to the appropriate transfer of information
       1. Takes into account privacy promises, sensitivity of data, value, and protection attached to its future use
11. Regulation of Privacy in the Commercial Sector
    1. FTC is the primary federal regulator of privacy in the commercial sector
       1. Powers mainly stem from Section 5 of the FTC act (unfair and deceptive practices)
       2. Criticized for being overly focused on notice and consent opportunities (no one reads policies, data transaction is everywhere, and choice is meaningless)
       3. David Vladeck is the new head of the FTC; focus on consumer rights
    2. FTC Report’s Recent Conclusions
       1. Current privacy law places too much burden on consumer to make privacy choices
       2. Must reexamine notion of harm in US law in connection with privacy, expand scope beyond economic or physical harm in order to catch privacy violators
    3. FTC’s Recommendations
       1. Industry should do more to preserve privacy on the front end
          1. Less notice/choice, less collection and less retention
       2. Align data promises with consumer’s reasonable expectation
          1. If using data in unexpected way, reasonably and prominently clarify use
       3. More transparency in data collection and use practices (online); clarification
          1. Who, what, and for what purpose is the data collection occurring
    4. Dep’t of Commerce is in conflict with the FTC
       1. Commerce promotes more self-regulation and increase in privacy policies
       2. FTC promotes stronger law, upfront efforts, greater consistency w/ consumer expectations, increased transparency
12. FTC Regulation Moving Forward
    1. Commercial regulation often criticized for being too sectoral
       1. However, FTC is still fairly responsive to specific needs of a specific sector since enforcement is so specifically focused and sectoral in nature
    2. Primary Objection to Sectoral Regulation
       1. There is note enough protection
       2. US privacy law is very bureaucratic, composed of notice that people do not cat on, understand, or read
       3. There is probably a need to move beyond notices (but not get rid of them entirely)
          1. Whether that is direct legislation, increased liability, it is unknown

III. Governance by Statutory Regulation

1. Sectoral Approach to Regulation of Commercial Entities
   1. Congress’s approach is “sectoral,” as each statute carves out a commercial sector and tailors itself to particular types of businesses and services
      1. Video is a fairly narrow sector
      2. Financial services is a much larger sector
      3. Some laws apply outside their own sector (health privacy goes to health care and businesses that partner with them - selling supplies to the hospital)
   2. United States does not have many comprehensive (omnibus) statutes regulating the private sector’s collection and use of personal information
      1. FTC Act is an example, very broad jurisdiction in commercial context
   3. Key question: “What is the sector and how broadly does it apply”
2. Video Privacy Protection Act (Entertainment records privacy)
   1. Prohibits videotape services providers from knowingly disclosing personal information without the individual’s written consent
      1. Private right of action exists under VPPA
      2. If more restrictive state law exists, must follow it (VPPA is a floor, not ceiling)
   2. Applies to any way in which you deliver a medium of video (tapes, DVD, online distribution), does not apply to transmission of video (cable)
      1. Requires a **physical medium** being transferred (ex. Applies to Netflix when a DVD is mailed, but not when a movie is streamed)
   3. Exceptions to Prohibited Disclosure:
      1. **Routine Business**: Disclosure of personal information is allowed if the disclosure is incident to ordinary course of business; delivery, bank, etc…
      2. **General Marketing**: General subject matter, not specific names, of videos may be disclosed if exclusively used to market goods and services directly to consumer
      3. **Specific Information** (w/ Opt-Out): Video providers can reveal names and addresses of customers if an opt-out opportunity is provided to consumers; cannot link names of videos to the specific information
3. Who is Regulated by the VPPA
   1. Act is most commonly triggered by law enforcement seeking records
      1. Failure to follow requirements of a subpoena or court order
      2. Instead, seek answers from video rental service providers
   2. *Dirkes v. Borough of Runnemede*
      1. Court holds that the VPPA is extended to police requests for information
      2. However, statue states it only applies to video service providers, so unless police perform video rentals or sales, court misinterprets the VPPA
   3. *Daniel v. Cantell*: Overturns *Dirkes* Decision
      1. The only person that can violate the VPPA under disclosure of information is the actual video tape service providers that disclose the information
      2. No VPPA claims against 3rd parties (e.g. police) who request the video information
4. Cable Communications Policy Act (Entertainment Records)
   1. Cable service providers cannot collect personally identifiable information about any cable subscriber without prior written or electronic consent of the subscribers
      1. Only **opt-in** statute that we have come across; Opt-in from the very start
      2. Shall not use the data other than as regulated by this statute
      3. Privileges information cable companies gather (what and when I watch), and it cannot be provided to anyone for marketing privileges, even with explicit consumer consent
   2. Exceptions to the CPPA:
      1. May disclose personal under certain circumstances
         1. **Legitimate business activity**: Collecting payment, reviewing credit qualification, vindication of legal claims, but not for marketing purposes
         2. Pursuant to a **court order** if the subscriber is notified
      2. May disclose subscriber names and addresses if the cable operator has provided the subscriber opportunity to prohibit/limit such disclosure
   3. Government Access to Cable Information
      1. Sensitivity about have government access our viewing records
      2. Requires government entity to provide **clear and convincing evidence** (pursuant to court order) **and** **notice** w/ an opportunity to object the entity’s claims
   4. PATRIOT Act
      1. Allows government entities open access to internet services records
      2. Still maintains higher standard for cable records
   5. Most Efficient, Protective, and Least Controversial Privacy Law in the US,
      1. Unique: Majority of rights under the statue are not eliminated through exceptions
         1. Efficient, few exceptions, and applies beyond privacy
      2. Effective: High protection, and inconsistent with any other privacy acts
         1. Narrow sector, and narrow data: Cable company knows location information (not very sensitive); payment information (credit card, checking); and viewing practices
5. Children’s Online Privacy Protection Act (Internet Use and Electronic Communication Privacy)
   1. Applies to website providers that target children under age 13, or that have actual knowledge that children under age 13 are using the site, and collect personal information
      1. Reason why many websites have warnings for no entry if U-13
      2. COPPA is unworkable in an online environment
   2. If you fall under this provision, cannot collect user information about children under age 13 without verifiable parent consent
      1. Presumes that if you have a credit card, you are over the age 13
         1. Websites that used to be free, began asking for cc #’s to proceed
         2. Website then ran the cc # (charging minimal amount) and transformed free credit websites into charge sites for children
      2. FTC first suggested to ask parents to mail a photocopy of drivers license
         1. Essentially leads parents to tell children to lie and forge verification
   3. Primary enforcement only against those that have affirmatively deceived the statute, or has severe non-compliance
      1. Safe Harbor: If an organization follows self-regulatory online guidelines that are approved by the FTC, COPPA requirements are deemed satisfied
6. Pharmatrack: ECPA and Online Privacy
   1. Pharmatrack uses cookies and clear jifs to gather information about users
      1. Cookies store data on your own computer about activity with a particular site
         1. Cookies used in 1990s for advertising delivery; remember what ads were show before and what you clicked on
      2. Clear jif places a small file on your webpage that watches and reports back to wherever it came from
         1. Ex. How long you look at page, what page next, what browser, what security (anything you could find out by accessing that person’s screen)
   2. Litigants claim that Pharmatrack (along with pharmaceutical companies) violated ECPA because it specifically intercepted communication without any authorization
      1. Pharmaceutical defendants received reports from Pharmatrack about who visited their websites, but say they did not consent to granular, individual level of data collection; court does not buy it
         1. If either party consented (pharmaceutical defendants or litigants) to the interception of data, interception would be legal
      2. Sufficient that pharmaceutical defendants were party to communications, and consented to monitoring service (did not need to know the details of the service)
   3. In a private cause of action, must show that the purpose for interception was for a crime or tortious act; but Pharmatcack was just fulfilling its k with pharmaceutical defendants
      1. Action fails and should never had made it to court; Use of ECPA fails
      2. Argument under stored communications act fails as well; individual computer is not a facility, and individual website is not a facility for which a service is provided
7. Facility or Service under ECPA: *Dyer v. Northwest Airlines Corporation*
   1. NW is providing data to government for tracking post 9/11 suspects or for testing these tracking procedures
      1. Complaint alleges that NW’s unauthorized disclosure of customers’ personal information constituted a violation of ECPA
   2. To sustain a claim under ECPA, must establish that NW provided either electronic communication services or remote computing services
      1. Provider of electronic communication services under ECPA are ISPs and telecommunications companies who carry internet traffic over their lines
      2. Does not cover businesses selling traditional products or services online (websites)
      3. **NW does not sell access to the internet itself, thus** **no ECPA violation**
8. Computer Fraud and Abuse Act
   1. Provides criminal and civil penalties for unauthorized access to **protected computers**
      1. Originally meant financial, government or health service computers, but act was amended to protect any computer connected to a network
      2. CFAA applies to ISPs and individual computers (all connected to networks)
   2. Federal omnibus privacy law that makes it illegal to gain unauthorized access to protected computers, or to exceed authorized access to a computer
      1. If someone accesses, or exceeds authorization or hacks the information, there are criminal violation and civil remedies
   3. To establish compensatory civil action or injunctive or equitable relief for damage suffered due to violation of the CFAA, damage must aggregate at least $5,000 value during any one year period to one or more individuals
      1. Damage cause must be **$5,000 to the plaintiff** in order to have cause of action
         1. Can aggregate loss across systems that belong to plaintiff in any one-year period (ex. IU can aggregate loss over all computers it owns, if breached by the same hacker)
      2. Plaintiff himself must have loss of at least $5,000, including not only value of stolen data, but the cost to fight or detect or remediate the breach
         1. Ex. paying $1,000 to hire someone to seal the breach that allows wrongful access is included
      3. Cannot aggregate across plaintiffs harmed by the same defendant and cannot aggregate harms caused from different attackers
         1. Ex. If one hacker effects several low cost attacks to different plaintiffs, cannot aggregate to establish one cause of action
         2. Ex. If 3 hackers do different harm worth $2,000, cannot aggregate to meet threshold of $5,000
      4. *Pharmatrack* and *Doubleclick* cases are almost never successful because they fail on the damages threshold of $5,000, difficult to establish an real damages to computer systems due to cookies
9. *Created Computing v. Getloaded.com LLC*
   1. Competitor tries to steal trade secrets by hacking to competitior’s website and downloading program code to reverse engineer it; CFAA violated?
      1. Original statute: If values of such use is not more than $5,000 for 1 yr., no liability
      2. Amended: Loss of any one year period aggregating to at least $5,000 in value
   2. Doesn’t matter, defendant loses under both interpretation of the statute
      1. Neither version supports a construction that would require proof of threshold being met form a single unauthorized access
      2. Argues that definition of damage under old statute refers to a single impairment leading to loss of $5,000, but multiple intrusions can lead to single impairment
   3. Damages threshold of the **CFFA has no “single act” requirement**
      1. Single victim may aggregate damages across one year period, no matter the number of individual acts perpetrated by the defendant
      2. Hacker that breaks in 100 times to the same system but only causes minimal damages no longer gets off because damages can aggregate to meet threshold
10. Megan Meier Case
    1. Mother of one of Megan’s classmates created a MySpace, pretended to be a boy, and then broke up with her publically, led to her suicide
       1. Criminal Claims Failed: Impersonating someone without commercial purpose is not against the law, no intent to cause injury
    2. One prosecutor brought claim arguing the CFAA should apply because the mother started an account, had authorized access to MySpace servers (computers), and it prohibited in its terms and conditions an account in other then your own name
       1. Argued that mother exceed authorized access to MySpace servers by violation of terms of service, and caused injury exceeding $5,000
    3. If terms of service/authorization can be set by a commercial entity, and if exceeding those terms constitutes a crime, then ISPs would be able to define crimes
       1. Actions was dismissed, no in the scope of CFAA
       2. Court will not let private ISP define contours of a criminal act
11. Telephone Consumer Protections Act
    1. Originally enacted to deal with unsolicited faxes
       1. With unsolicited calls, no economic harm bc you can just hang up
       2. With faxes, consumer/receiver pays certain costs (paper, ink, etc…)
          1. Fax costs were becoming astronomical, and tied up fax machines
          2. TCPA effectively prohibited unsolicited public use of faxes
    2. TCPA also incorporates opt-in, no call lists for telemarketing
       1. No telemarketing at certain times, regulations on minutes, and robo-calling
       2. Prior to the opt-in “do not call” registry being implemented into the TCPA, telemarketing was the biggest privacy driver
12. Can-Spam Act of 2003
    1. Unsolicited commercial email required to be advertised and such, and required to provide an unsubscribe list; reasons behind act include:
       1. Unsolicited commercial email had a fair amount of sexually explicit material, and children could have been exposed w/o any parental knowledge or consent
       2. Most common use of unsolicited commercial email was sending malicious code or viruses, vector by which people were attacking computers (strongest argument)
          1. Email is arguably like a fax, costs behind storage and costs of printing
          2. 90% of trillion emails received/day are junk mail, w/ more than half having malicious effects/phishing emails
    2. Can-Spam Act applies to any commercial email
       1. FTC complicated interpretation of what is commercial
       2. If entities are unsure if they are sending out a commercial email, there are potential consequences if they do indeed send out a commercial email with no unsubscribe option and are not advertised as such
          1. Ex. Law firms sending out email notifying a legal change, assuming that the firm wants to foster more business (commercial or not?)
    3. Can-Spam Act failed to address the bulk of the problem
       1. If someone is already committing a crime by sending malicious emails, why would they follow the FTC’s labeling requirements under the Act
       2. Volume of span increases exponentially each year, and has no reasonable effect besides slight liability for companies failing to follow some provision
          1. Still no liability for criminals who use spam
       3. Also created a system where unsolicited commercial emails are considered as legitimate by consumers, as long as it is labeled as such
          1. Criminals now use unsubscribe buttons to launch viruses/harvest addresses
    4. FTC study concluded that “do-not-email” lists (ala do-not-call lists) were **not feasible** 
       1. If individuals are already committing a felony, they are not to going to check a do-not-send list before sending off hazardous emails
       2. Creating a list of in-use, good email addresses would create a huge target that every hacker would be after (list of real addresses not being inundated with spam)
          1. List could not be secured effectively
       3. Do-not-call lists are enforced by comparing the do-not-call list and the telemarketer’s list, and striking the names that appear on both lists
          1. If done for the internet, spammers and hackers would line up for the opportunity to review these lists; just not a feasible security measure
    5. Legitimate commercial email is sent to people who are targeted after information about their online habits is collected and reviewed
       1. FTC is considering an opt-out for any online-profiling
       2. If consumers did not want to receive those commercial emails, could place a cookie indicating that you did not want to be profiled, and every legitimate company would have to check and not profile your information
          1. Legit spammers would have less incentive bc they have no info on you
       3. Only spam you would receive would be felonious and you could just block it
          1. Unlike today where some spam is legitimate and some is malicious, so you cannot do an overall comprehensive block of spam
    6. Act preempts more restrictive state laws
       1. Tension between state and federal legislation;
          1. Informational so inherently national/global, no need for state law
          2. Conversely, states say that countries are too slow to react, states are needed for urgent reaction
       2. Federal government is bi-polar; allows states to enact stronger laws, but then with things like Can-Spam Act, they pre-empt any state law on the issue

***C. Data Security***

1. Database Industry
   1. Database industry consists of companies that compile, analyze and trade personal data
      1. Referred to as **data brokers**
   2. Ex. Acxiom; provides information to marketers for profiling consumers, manages credit records, sells data for background checks, and provides data to government agencies
      1. Other databases include Choicepoint, LexisNexis, etc…
2. Data Security Breaches
   1. Includes where Data Security Companies have been defrauded (*See* Choicepoint)
      1. Fraudulent applicant buys subscription to the database information by signing up under a fraudulent company name; or gained entry through sheer force hacking
   2. Cate disagrees with book, **security breaches in large data companies are not a big deal**
      1. Companies are very good at what they do
      2. Even if they lose 250,000 records/year that is infinitely tiny given the scope of information they retain
   3. Definition of data breach includes losing thumb drives with your data on it, or someone broke into your system and gained access to records
      1. Ex. VA contract EE took an external hard drive with records of every veteran, and teenagers ended up stealing his computer/information
      2. Computer was found, and information was never looked at, but government spent $70 million informing veterans that their information may have been compromised
   4. Majority of data breaches do note end up as breaches; such as in the VA incident
      1. Some data breaches could be very serious, but numbers that indicate 758 million records being compromised are usually part of equipment stolen or lost
      2. Ex. IU sends a file via fed ex, but fed ex left it on the doorstop and it disappeared; even iif it is found later (still sealed), it is considered a data breach
   5. State and federal government do not want to take comprehensive action, because in most circumstances these “breaches” are not a big deal, but don’t want to do nothing
      1. Government adopts an in-between, sending letters informing individuals there was as breach, but there is nothing they can do about it
3. Choicepoint Security Breach
   1. Identity theft crime ring set up fake businesses and signed up to received ChoicePoint data
      1. Personal information, including names, addresses, and SSNs of other 145,000 people were improperly accessed, and over 700 were victims of identity theft
   2. FTC fined ChoicePoint 10 million dollars, largest fine ever imposed by the FTC
      1. Imposed a 5 million dollar restitution, so people who were injured and might have had their information compromised could be reimbursed
4. There have been almost zero reported injuries due to data breaches
   1. Statistically, there is just little injury that stems out of data breaches
      1. Ex. The $5 million ChoicePoint restitution fund, only paid out $141,000 to 131 claimants (3 years later), every claim received restitution
      2. 163,000 people involved in breach and only 131 presented receipts/valid claims to the FTC and got money back
   2. U.S. Government Accountability Office studied 24 largest breaches in past 5 years
      1. Only 3 of the 24 reported any evidence of use of the data, and only one breach resulted in identity theft
      2. Back to the VA breach, and the misuse rate for fraud of SSN was 1/1010, where the national range for fraud is 1/1020
   3. As a legal matter, 180 class action suits have been filed based on data breach, and every one of them has failed, classes were not certified and no damage found
5. Civil Liability for Data Breaches: *Pisciotta v. Old National Bancorp*
   1. There is a break in at the NCR’s hosting facility that maintains ONV’s website
   2. File a class action suit, but no individual in the class has evidence of any harm
      1. Plaintiffs sought to claim that they had increased monitoring risk, fear, and would have to spend more time reviewing credit reports; argument controversially fails
      2. Solves argues it is akin to losing a key to your house and not sleeping safe until locks change, but courts reject this argument
   3. No chance for strict liability to flow out of data breach cases
      1. Do not want to enrich plaintiffs and attorneys when no harm is actually done in certain situations
      2. There should be other ways to enhance accountability and data maintenance beyond the individual
   4. On the federal level, no general notification statute, but there is a growing movement through federal regulation and FTC enforcement to provide notification in the event that health institutions, and financial institution are required to notify if they suffer a breach
      1. FTC is aggressive in this area, utilizing **unfairness power** to impose liability
   5. Majority of states (44/50) have a notification statute if a data breach occurs (CA was 1st)
      1. Basically everyone is under duty to notify of a data breach (even in states that don’t require it under statute, it is generally done anyways)

***D. Health and Genetic Privacy***

I. Confidentiality of Medical Information

1. Distinguishing 3 Key Points on Confidentiality of Health Information
   1. Evidentiary Privilege of Non-disclosure
      1. Physician-patient privilege
   2. Confidentiality Tort
      1. Within the context of physician-patient relationship (whether under a statute or Hippocratic oath), you can sue the physician who discloses personal information about you and causes harm
         1. The tort is special to physicians (and other specific professions)
      2. Separate from a public disclosure-private interest tort which requires the disclosure to be shocking to the conscious
         1. For the purposes of this confidentiality tort, physician leaked information about you is assumed to be shocking
         2. There is no 1st amendment defense for the physician, because there is no 1st amendment right to share information about the patient’s medical history
   3. Disclosure Requirements
      1. Physicians are **required** to disclose information in certain situations
      2. Duty of psychotherapists to warn someone who may be in danger, duty to report about hepatitis, communicable diseases, victims of abuse/neglect, AIDS/HIV
      3. Places health care providers in a catch-22
         1. Patient can stop physicians from disclosing information and can be sued for certain disclosures
         2. Physicians can also go to jail if they fail to disclose information under specific circumstances where disclosure is required
2. Hippocratic Oath: Ethical Rules for Professional Conduct
   1. Concept of physician confidentiality is very old, and recognized widely by the AMA, the canon of medical ethics, state medical societies an din the law
   2. Considering scope of health care policies, ethical guidelines implicates more sectors then just physicians and health care providers (IT, insurance, etc…)
3. Evidentiary Privileges of Physician-Patient Relationship
   1. Under US law, patients (the non-professional in the relationship) have the right to waive privilege, but the professional (physician and other health care providers) remains bound by the privilege and is not permitted to waive it without the holder’s consent
      1. Privilege is waived expressly or through patient’s conduct (voluntary knowing disclosure waives a privilege)
   2. Certain circumstances where privilege does not apply
      1. If communication is made in furtherance of a crime, fraud or misconduct, then it is not privileged (crime-fraud exception)
      2. If a patient sues a physician, physician can testify as to confidential matters in suit
4. Existence of Privilege: *Jaffee v. Redmond* 
   1. Confidential communications between a licensed therapist and her patients in the course of diagnosis or treatment is protected from compelled disclosure
      1. Even if notes are relevant in determining the truth (what D really remember about the incident) for a wrongful death suit, not as important as protecting privilege
   2. Without privilege people will less likely go get help, and having the psychologically disturbed received help is a higher societal priority then people who may find dispositive evidence in these records
      1. Court views mental health as a transcendent public good
      2. Court takes potentially relevant information, but makes it off limits by calculating the public interest is better served by applying privilege
   3. Dissent argues that by protecting rights of therapy over rights of people seeking records, they are deny access to potentially relevant set of records
      1. We might all benefit from talking about our problems with our friend, but there is generally no privilege protecting them

II. Tort Liability for Disclosure of Patient Information

1. Tort for Breach of Confidentiality Duty: *McCormick v. England* 
   1. **Actionable tort** exists for a physician’s **breach of the duty** to maintain confidences of a patient where there is **no compelling public interest** or other justification for disclosure
      1. Does not mean you can never reveal information, but if your calculation is wrong and there was no justification, physician is liable for the tort claim ($$$)
      2. Here, physician wrote a letter for a custody proceeding w/ significant disclosure or personal information
   2. If this was a privilege case, patient has a right to keep testimony out of the proceedings (government can’t compel testimony), but no right to get paid for broken privilege
      1. This case focuses on tort action seeking compensation for breach of confidence
   3. Breach of confidentiality (privilege not to be compelled to testify) and confidentiality tort (payment for breaking confidence) is distinct from invasion of privacy (public disclosure of private facts) tort
      1. Invasion of privacy focuses on conduct that is highly offensives and likely to cause serious mental injury, no consistent with duty attached to confidential relationship
      2. Invasion of privacy tort focuses on content – disclosure of facts with no legitimate public interest, rater than the source of information
2. 3rd Party Inducing Breach of Confidentiality: *Hammonds v. Aetna Casualty & Surety Co.* 
   1. When a doctor agrees to treat a patient, and consensual relationship forms between physician and patient, two (2) jural obligation simultaneously assumed by the doctor
      1. Implied K: Patient hopes to be cured and doctor assumes he will be compensated
      2. Due to the K, any confidential information through relationship will not be released unless with patient’s consent
   2. If you fraudulently induce a physician to disclose information in violation of state confidentiality tort, you will be liable in place of, or in addition to the physician
      1. D knew or reasonably should have known of the physician-patient relationship
      2. D intended to induce the physician to disclose info about the patient, or should have anticipated that this actions would induce physician’s disclosure; and
      3. D did not reasonably believe that the physician could disclose that info to the defendant without violation duty of confidentiality owed to patient
   3. R2d: Individual or entity that knowingly assists a fiduciary in committing a breach of trust is himself guilty of tortious conduct; **Fiduciary relationship** **btwn physician and patient**
      1. Ex. Insurance companies inducing a doctor to reveal confidential information gained through patient-physician relationship to use in pending litigation against the patient, under the pretext that patient was contemplating malpractice suit
   4. R2d: One standing in a fiduciary relation with another is subject to liability to other for harm resulting from a breach of (confidential) duty imposed by the relation
3. Holding Hospital Liable for Breach of Confidentiality: *Biddle v. Warren*
   1. Duty of confidentiality does not deal with acting in the best interest of the patient
      1. Unless serving a compelling public purpose, the balance of interest do not favor disclosure and breach of confidentiality
   2. Tort of confidentiality is not concerned with the harm caused
      1. Focuses on who discloses the information and whether it was derived from a confidential relationship
   3. Lawrence Gotsin argues that the rule of confidentiality does not work in modern information society; something better than the confidentiality tort is needed

III. Tort Liability for Failure to Disclose Patient Information

1. Disclosure Obligations: *Tarasoff v. Regents of University of California*
   1. In the course of a privileged therapist-physician relationship, if the therapist learns of a credible threat to a third party, **legal duty to disclose exists** 
      1. Generally, disclosure focuses on public interests (spread of disease), but this focuses on private interests (obligation to 3rd party, no one else in harm)
   2. If patient harms someone else (not the target you were made aware of) on the way to the individual to which physician owes the duty, there is no liability to the other harmed guy
   3. Liability only exists under non-disclosure for identified 3rd party victims
      1. Psychotherapy profession strongly opposed liabliity; concern is over creating a legal obligation (when most already disclosed these warnings anyways)
   4. Duty of Confidentiality can only be violated w/o impunity under certain circumstances
      1. Required to relay information of a credible threat to an identifiable 3rd party
         1. Tarasoff Tort Liability: Failed to warn when you should have?
         2. Confidentiality Tort: Warn (and disclose info) when you should **not** have
   5. Disclosure of threat to identifiable 3rd party is the biggest of the disclosure requirements because it is the vaguest and could apply to many setting
2. Disclosure Obligation for a General Threat: *McIntosh v. Milano*
   1. Duty of Disclosure may be founded in either:
      1. Statute: Usually related to a general interest
      2. *Tarasoff*: Identifiable 3rd party
      3. *Milano*: Unidentified 3rd party, but a theoretical general obligation to protect welfare of the community (without being provided shelter of a state statute)
   2. If there is a general threat, practitioner has a duty to protect the welfare of the community
      1. Analogous to the obligation a physician has to warn 3rd parties of infectious diseases, but that is duty owed generally and under statue
         1. Notify the government (statute) and satisfy the obligation for the broad public protection obligation bc it is not linked to a specific victim
      2. *Milano* requies a broader obligation
3. Duty to Warn About Relatives’ Genetic Conditions: *Pate v. Threlkel* 
   1. When physicians treat someone for a condition with a genetic component that might get passed down to their children, no duty to the children
      1. Genetics is like craps, know the odds but there is no certainty
      2. May be warning about something that never materializes
      3. No identifiable victim (unlike *Tarasoff*); unsure which child has the defect
   2. Physicians **duty is to the patient**
      1. Obliged to tell patient to warn your children about this defect
   3. **Duty is** **not to the person at most risk** of the condition, because of confidentiality
      1. Minority approach: make sure that patient understands that their offspring might be at risk for the condition
         1. But this makes no sense, don’t tell HIV positive to just have safe sex
      2. In other states, duty is to the offspring and no duty of confidentiality to the patient
   4. Some states establish duty of confidentiality to the patient for genetic diseases, but eliminates that duty of confidentiality for infectious diseases
4. Robert Gellman: Defining physician responsibility with respect to patient privacy
   1. These responsibilities should be defined by legislatures, not the courts
   2. If we are dealing with complicated, interesting rights, and trying to protect medical privacy, this should not be handled by courts after the fact
      1. Under the court decisions, standards will be different from state to state
      2. This is a policy matter that should be thought through by legislators

IV. Health Insurance Portability & Accountability Act (HIPPA)

1. Introduction
   1. Until 1999, health privacy was a state matter, and states conflicted with one another on evidentiary privilege, confidentiality tort, and disclosure requirements
   2. Federal action for health privacy was established under HIPPA (started in 1996)
      1. Guidelines for HIPPA established first under Clinton’s privacy rules, but they did not go into effect until they were amended by the Bush administration
2. Entities Subject to HIPPA Regulations
   1. Regulations apply to Covered Entities
      1. **Health care providers**: provider of medical or health services and any other person or organization who furnishes bills or is paid for health care in normal course of business (physicians, hospital, pharmacists, etc…)
      2. **Health plans**: Individual or group plan that provides, or pays the costs of medical care (health insurers and HMOs)
      3. **Health care clearinghouses**: public or private entity that processes health information into various formats – either into standard format or into specialized formats for needs of specific entities (billing organizations)
   2. Regulations **do not apply** to Non-Covered entities
      1. Websites: Even if providing medical information, not covered my HIPPA
         1. More health info is gotten from the web then from doctors
      2. Pharmaceutical Companies
         1. Don’t charge, don’t service patients directly, and don’t provide health care
      3. Does not apply to many organizations where health info is exchanged
   3. Hybrid Entities
      1. Entities may provide a variety of products and services, only some of which pertain to health care; less stringently regulated then covered entities
      2. Only the sector of the organization that would be considered a covered entity has to comply with HIPPA (Ex. IU psychological/medical centers are covered, rest is not)
3. Type of Information and Records Covered (If it is a covered entity)
   1. **Individually Identifiable Health Information**:
      1. Records have to be electronic at some point;
         1. Prohibits IIHI whether oral or recorded in any form/medium
      2. Limited to information that is created or received by the health care provider, plan, or clearinghouse; and
      3. Information must be for the provision of health care that identifies the individual or reasonably can identify the individual
         1. Does not specify that it has to be a living individual (ex. uncle that dies without paying a bill is still covered information)
   2. Requires that at some point in the record’s life span, the record was electronic
      1. Physician hand writes a note, and is transcribed to the computer
      2. When sending bills, they may be typed, but when sent electronically, the whole stream of records is covered
   3. Everything in the medical or insurance practice is essentially covered
      1. Only exception would be doctors living out in the range (Dr. Quinn Medicine Woman), where there would be no electronic transmissions
4. Privacy Protections under HIPPA: Authorization
   1. **Acknowledgment**: Treatment or payment or health care operations does not require an explicit written document, only requires an acknowledgment
      1. In order to treat a patient, must supply notice about physician privacy practice, describe a patient’s legal rights, and the patient must sign a statement acknowledging receipt of this information
      2. Alternatively, if the patient refuses to sign the statement, he must sign an acknowledgment that says he refused to sign the privacy practice statement; if he refuses to sign this acknowledgment, 2 witnesses are required to say that he refused to sign the statement or the acknowledgment
      3. **No consent is required** **for treatment or payment or health care operations; but there must be an acknowledgment of presence of the notice** 
         1. Acknowledgments/Statements must be maintained for 6 years after the date of last treatment of the patient
         2. Not required under statute, just a very bureaucratic rule
         3. Must acknowledge receiving notice
   2. **Consent:** For Everything Else
      1. Everything else that is not for treatment, payment or a health care operation requires opt-in, written consent
   3. **Agreement**: Uses carved out of consent, uses for directory information
      1. If you cannot use directory information without consent, and an individual shows up and asks if that person is at the hospital, cannot tell them
         1. Cannot disclose answers to “where is he?”; “what is his condition?”
      2. This is Opt-out consent
         1. Covered entities can use this directory information to tell people condition, status, and location unless patient tells entities not to use that information
         2. Entities are required to give notice that they have opt-out opportunity
   4. HIPPA is the triumph of US privacy policies
      1. Three (3) different types of consent – acknowledgment, consent, agreement – for information in one setting, and each requires their own notice
         1. Notice of Acknowledgment
         2. Notice if you are agreeing to something
         3. Notice to agree to use directory information
      2. Each of these notices must be on separate pieces of paper
5. Privacy Protection under HIPPA: Marketing
   1. Consent required for use & disclosure of health data for marketing items and services
   2. If covered entities want to provide a person’s health data to a 3rd party who wants to peddle goods or services, must first obtain that person’s consent
      1. Consent is required even if the marketing is done by the conversed entity or one of its divisions
   3. Excluded from definition of marketing is the covered entity’s own provision of health-related services and products
      1. Covered entity can use an individual’s health info without consent to sell services or products as long as related to health care operation
      2. If no related to health care operation, requires consent
6. Exceptions
   1. Non-authorized uses & disclosures of health info that can be used or disclosed w/o consent
      1. Required by law
      2. Public health activities
      3. Regarding victims of abuse, neglect, or domestic violence (under certain circumstances)
      4. Health oversight activities
      5. Judicial and administrative proceedings
      6. Law enforcement purposes
      7. Avert a serious threat to health or safety
      8. For specialized government function
      9. Workers’ compensation
   2. Health information may be disclosed to law enforcement officials without consent or authorization if required by a court order, warrant, or subpoena, or if it is for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person

***E. International Privacy Law***

I. Introduction

1. Reasons for difference in privacy approaches between US and Europe
   1. In the US, primary fixation of privacy focuses on the government
      1. Historical perception of a general distrust or concern over government
      2. 4th amendment is a governmental privacy right, only aims to protect individual rights against the government (quintessential American view of privacy)
   2. Polling data indicates otherwise, government is a concern, but telemarketing is the biggest concern among people; government rarely makes the top 10
      1. Oversimplification to say the American approach to privacy is due to government
   3. Experience of the 1940s and 1950s which explains Europe’s view on privacy
      1. Nazis utilized national registers (id cards, birth and marriage records) to determine who to discriminate against; vast non-automated data use
      2. Stasi in East Germany collected complete dossiers on every person in the country, including mason jars of every person for scents to catch wall jumpers
2. Differences in Privacy Legislation
   1. European privacy law is “omnibus,” where one statute typically regulate the processing of personal information in public and private sectors alike
      1. Outside Europe, other countries moving towards comprehensive privacy laws
   2. US privacy is “sectoral,” where a series of narrower laws focus on specific sectors of the economy or certain technologies
3. Basis of European Privacy Law
   1. Shaped by the traditional role of the Council of Europe and Article 8 (1950)
      1. Established privacy protection as a critical human rights claim in postwar Europe
   2. Today, central focus of European privacy law is the EU’s Data Protection Directive
      1. Establishes a basic legislative framework for the processing of personal information in the EU
   3. Data protection is frequently used to describe privacy protection in the European context, and concept of private life or domain, is key in Euro-informational privacy

II. Privacy Protection in Europe

1. Two Western Culture on Privacy: Dignity (EU) v. Liberty (US) – James Whitman
   1. Europeans reverting to dignity interest, and hyper sensitivity to reputation as a marker of status in society (back to royal history of Europe) as focus for privacy
      1. Historical hierarchies were based on colors, etc…and the stratification of society is the basis of European informational privacy law today
   2. Maintain hierarchies today through protection of privacy (rather than duels or clothes)
      1. In Europe, there are hundreds of successful cases where celebrities sue to protect their privacy, and dignity and social status is protected
   3. Controversially argue that the Nazis brought the change to European privacy
      1. Nazis leveled society, bringing law and mechanization into the process, made social status official rather than a social conception
      2. Taught people how important data was to maintaining position in society
   4. When conducting polls, Euros and US citizen react almost identically
      1. US is more tolerant of direct marketing, but the general worries are the same
      2. Privacy laws are different, but unsure why
2. European data protection focuses on protecting the data, not the individual
   1. Examines the accuracy, completeness, timeliness, integrity of data
      1. Privacy is the right of the individual in the US
      2. Europe examines privacy as distinct from data
   2. Dangerous to assume that data protection = privacy
      1. Protections are different as to data protection and to privacy, but Cate is unsure as to the difference
      2. Quartering soldiers in your home deals with privacy, but presenting a license to fly is a data interest
      3. Profiling is a data protection interest, patting people down is a privacy interest
3. OECD Privacy Guidelines
   1. Organization for Economic Cooperation and Development is composed of the US and Euro countries, and they issued guidelines for privacy protection in the transfer of personal info across national borders
      1. Not just about privacy, but is driven by economic concerns about free flow of data
      2. Argues that if nations could agree on some global principles, that would help facilitate the movement of data and preserve strength of the economy
      3. Int’l privacy agreements including both the US and EU is rare, typically only one of the parties signs due to disagreements
         1. Europe has been part of many agreements that the US was not
   2. OECD’s eight (8) principles regarding processing of personal data are based on US privacy law, establishing comprehensive protection and a standard for good privacy law:
      1. Collection Limitation
         1. Some limit on what information is collected, based upon what is necessary, **consent**, or any guiding principle
         2. Acts as a superseding principle establishing limits, does not advocate for a comprehensive, vacuum cleaner approach
         3. Collection should be done legally, fairly, and where possible, with the consent of the data target
         4. **No secret data systems, and there must be limits to data collection**
      2. Data quality
         1. Data should be relevant, accurate, and up to date for whatever purpose you intend to use it
      3. Purpose Specification
         1. There should be some explicit statement of purpose no later than at the time of data collection, and data collection should be limited either to that specific purpose, or purposes not incompatible with that purpose
         2. Using data for compatible purposes does not require additional consent or consideration
         3. Ex. Under the GLB, you expect to be sold an item associated with the bank, but attempting to sell you a non-financial 3rd party item; non-compatible
         4. Ex. Collecting financial transaction info to find a terrorist; compatible
      4. Use Limitation
         1. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle, except:
            1. With the consent of the data subject; or
            2. By the authority of law
      5. Security Safeguards
         1. Must provide reasonable safeguards against risk of loss, unauthorized access, destruction, use, modification, or disclosure of data
      6. Openness
         1. Transparency principle
         2. No secret data collection and use
      7. Individual Participation
         1. Individuals have a right to know that data is collected about them generally, to have access to that data, and to be able to object or have it corrected
         2. Ex. FRCA: Consumers can dispute data if inaccurate unless the provider can prove it is accurate, place a statement in your record if disputed
      8. Accountability
         1. If you do not follow the guidelines, you should be held accountable, even if no harm is caused
         2. Required to follow laws irrespective if you plan to cause harm
   3. Guidelines are nonbinding on members of the OECD, but still have significant impact on development of national law (Cable Act of 1984 influenced by OECD)
4. European Convention on Human Rights Article 8
   1. Everyone has the fundamental human right to respect for private and family life, his home, and his correspondence
      1. Akin to US 4th amendment concept, traditional view of privacy (W&B)
      2. Private life must mean something in addition, beyond how an individual acts with their family (autonomy, dignity?)
   2. Private actors may not interfere with this right, but a public authority may have the opportunity to interfere with the exercise of this right if it entitled to under the law, and is necessary in a democratic society, in the interest of national security, public safely, or the economic well-being of the country, etc…
      1. Requires a legal provision clarifying what other right is being protected, and protection must be necessary (legal basis and practical basis)
5. Privacy and the Media: *Von Hannover v. Germany*
   1. Concept of private life extends to aspects relating to personal identity, such as a person’s name or a person’s picture, guaranteeing physical and psychological integrity
      1. Publication by various magazines of photos of the individual in her daily life by herself or with others falls within scope of her private life
      2. Anyone, even if they are known to the public must be able to enjoy a legitimate expectation of protection of and respect of their private life
   2. Germany did not strike a fair balance in the competing interests of privacy and free expression (Article 10), and violated Article 8 by failing to provide right to private life
      1. Balancing these rights swings on whether the information delivered is to a debate of general interest (though undefined)
      2. Difficult to bring this action in the US, but common in Europe
6. Privacy and Place: *Niemitz v. Germany*
   1. Involves a search of a lawyer’s office
   2. Private life and home, under Article 8, is extended to certain professional or business activities or premises (though issue is a business, location is not dispositive)
7. US v. Europe Approaches: *Copland v. United Kingdom*
   1. College suspects an affair between two of its EEs, but the subsequent investigation is a violation of privacy in the UK (nothing suggests it is a legitimate suspicion)
      1. Did not monitor content, deputy principle just gets copies of the phone bills to see who talked to whom, and for how long
         1. Monitoring of content is allowed in US w/ single party consent (FCA)
      2. Receives computer logs of header information, frequency and sites visited
         1. In US there would be no protection under 3rd party doctrine
      3. The UK law in place authorizes the college to do anything necessary as a public institution to maintain security of its systems, but no specific policy that allows anything further in the context of the college
         1. Under the US, hard to think of a cause of action for the EE under suspicion
         2. No constitutional or statutory interest, don’t need special needs doctrine
         3. Another avenue in the US to establish no reasonable expectation of privacy in the work place
   2. Article 8 clearly applies
      1. Business premises are covered by Article 8 private life and correspondence
         1. Private life and correspondence even apply to business life and business correspondence; work-emails are covered as well
      2. College gave no warning that the calls would be liable to review and investigation, so the EE had a reasonable expectation of privacy (extended to e-mail as well)
         1. Can receive bills for accounting principles, but cannot use them for investigatory purposes
         2. Whether you already had the records in your possession is irrelevant if you intend to use them for another purpose
         3. Storing information for a period of time in order to use it later for a different use triggers Article 8 protection (after receiving data, you have certain period to possess it, and subsequently storing it is a violation)
         4. Mere storage or presence of data in the file, even without consultation would have triggered an Article 8 violation
      3. In accordance with the law (recalling earlier cases), it is implied that there must be a measure of legal protection in domestic law against arbitrary interference by authorities with the rights safeguarded by Article 8
         1. Under US law, if congress authorizes use, you can use the data
         2. Europe establishes that there must be legislative authorization and it must meet some basic standard of human rights (balancing existence of legal obligation and the qualify of law being complied with)
   3. The college is authorized under the organic statute to act in manners necessary and expedient for its operation, but court argues that is too vague
      1. The organic statute fails the quality test, and because no other domestic regulation is relevant at the time, interference was not in accordance to Article 8
      2. Government says there was no harm, but court awards 3,000 euros (1/5 damages for surveilling content, and heading info) and 6,000 euros for costs and expenses
8. Summary of European v. US approaches to Privacy
   1. Europe: expectations of privacy exist in work, public, and at home
      1. In order to take away privacy, requires consent, notice, or law
      2. If consent is not meaningful, not valid under European law
      3. Consent is generally not enforceable in an employment setting, imbalanced and illusory consent (EEs have no choice but to comply)
   2. Ex. Finnish law explicitly states you cannot consent to waiving privacy right in an employment setting (American Airlines: kosher meals info is religion, and sensitive data)
   3. US: there is no privacy expectation to start with (work or at home)
      1. Notice or consent are not necessarily required
      2. Consent is always meaningful, even if people do not know what they are reading and it is often meaningless
   4. *Epifke v. Human Science*:French ER has an EE downloading porn on work computer
      1. In US, under EEOC there may be obligation to block that, and ER is within rights to fire you
      2. French high court said it was unreasonable to search the work computer and to fire the EE, there exists a constitutional right in a computer even though access is paid for by the ER, and the policy indicates it is only for work
   5. *Nikon*: EE fired for running a competing business on a work computer (stole trade secrets)
      1. ER looked at the EEs computer to find evidence to confirm their suspicions
      2. High court found this violated EEs privacy

III. EU Data Protection Directive

1. Establishes a complete union within the EU
   1. No longer just economic, establishes a cultural, legal, and regulatory unity
      1. Instructed nation-state, member governments to set forth certain legal requirements
      2. Member states are usually free to achieve those requirements in several ways, as long as they are achieved
   2. 1995: Directive was formally adopted; meant to protect individuals and was interested in insuring privacy did not become an obstacle for data in a unified Europe
      1. Implemented by nation states by 1998, and then went in to force in 2001
   3. Certain nations adopt it in tact, treated directive as a model statute
      1. Most nation-states adjusted the model statute slightly (work for lawyers in the individual countries to figure out what the law is)
      2. Directive is **not** a statute, it is seen as a blueprint for EU data protection & privacy
         1. Directive has no legal force on its own
         2. Look to the individual nation’s laws, not the directive, for regulation
   4. Enforcement of the EU directive
      1. Because it was an omnibus privacy law, dealt with changing world
      2. Had to revise the directives as technology was changing, big databases assembled without public access
2. Scope of the Directive:
   1. Imposes obligations on the processors of personal data
      1. Requires technical security/notification of individuals whose data is being collected
         1. W/o the data subject’s permission, personal data is not subject to processing
      2. Gives individuals substantial rights to control the use of data about themselves
   2. Personal Data: information relating to an identified or identifiable natural person
      1. Identifiable person: one who can be identified, directly or indirectly, in reference to an identification number, or to one or more factors specific to him
         1. Natural person does not have to be alive to be protected under directive
      2. Directive protects all data that can be linked to a natural person (individual, not a corporation); sound recording, written, video, etc…
         1. EE’s business email in the context of his job is identifiable bc there is a sender and receiver, protected
      3. IP Addresses are identifiable because they can be traced back to see who logged in and what IP address was assigned (can identify IP address w/ login info)
         1. All web based information is personally identifiable because you can eventually figure out who went where
   3. Processing: directive focuses on anything that can be done with data
      1. Copying, transmitting, destroying, receiving, sending, etc…
         1. Ex. Destroying a data center is considered processing data
      2. Comprehensive term that leads to a processor
         1. Controller is the party whose data is processed, controls the data processing
         2. Ex. Lawyer (controller) tell secretary (processor) to send email
      3. Does apply to normal government activities (licensing, benefits, etc…)
         1. Only exceptions to government compliance of the EU Directive is below
      4. Not limited to commercial entities, not for profit are applicable to directive as well
         1. Applicable to public and private sectors
         2. Does apply to normal gov. activities, only the exceptions do not apply
3. Directive does not apply to:
   1. Areas of activity outside legal competence of the EU at time it was adopted
      1. Public security, criminal law, national security, defense
      2. Government may be under certain privacy laws in those areas, but the directive does not compel them in those areas
   2. Processing of personal data by a natural person in the course of a purely personal or household activity
      1. Ex. writing a list on a refrigerator, do not have to comply with the directive
      2. Ex. If girl scouts come to the door and you buy cookies and give them your address, that is commercial activity and is clearly processing data (girl scouts are collecting data, and processing it, and must follow the directive)
   3. No exception for company data (only natural persons are covered under the ED)
4. Directive creates set of legal rights and mechanisms for enforcement
   1. Implements all OECD Privacy guidelines
      1. Cannot collect information without consent, individuals have right to access data, provide right to rectification or objection, etc…
      2. Generally, consent is required up-front (opt-in)
   2. Before using an individual’s information, general consent is not required, individuals can consent to certain things, object to others
      1. There is an individual right to objection for each act of processing
      2. Ex. collection, recording, organization, storing, retrieval, consultation, etc…
   3. Most striking protection is right not to be subject to certain automated decisions
      1. Requires explicit consent for automated decisions
      2. Machine based decisions require some form of human involvement
      3. Ex. Applying for credit in EU, and notifies you that you will be subject to automated decision, if you consent the right no longer applies
5. Directive Data Collection Commissioners/Supervisory Authority
   1. Every EU member state is required to have its own independent data protection authority, who have supervisory authority and are data collection commissioners
      1. Process registrations for data processing
      2. Entities cannot process data without registering with the supervisory authority
   2. Cannot carry out data processing without registering, and individuals get access to registration information
      1. Registries are public, and can see data protection officials by name
      2. Ex. Cannot collect credit information without going to the supervisory authority and registering and identifying the controller by name
   3. Supervisory authority have right of investigation and right to issue penalties
      1. Must have the power to investigate complaints and issue dissuasive penalties (large enough to deter future behavior)
      2. These authorities can come into your business and ask for your records
      3. Ex. Spain can issue investigation and fine through supervisory authority, and commissioner keeps own fines to fund the office
   4. Also helps interpret and apply the directive
      1. Do not offer regulations, but do provide advisory opinion individuals can consult that are integral to interpreting the directive
   5. Supervisory authorities meet together in Article 29 working party to issue interpretations
      1. Are part of the government, yet independent from it
         1. Not party to the executive branch, and cannot report to head of government
         2. Not controlled by president or prim minister
      2. FTC recognized as an independent supervisory authority for the first time this yr
      3. Data-protection is being negotiated by non-governmental representatives
6. Adequate level of protection under the EU Directive (Article 25)
   1. Restricts the flow of data outside the EU to countries that lack adequate data protection
   2. Adequacy is subject to some exceptions/derogations (Article 26)
      1. Personal data can be transferred to third-party country without adequate protection if there is informed consent, and the subject is described the perils that their data will face in an inadequate country
         1. Cannot use this with EEs, or anyone with no real chance to not consent
      2. Overriding individual interest
         1. Ex. someone is hurt and hospital records are necessary, but they are unconscious, overriding personal interest
   3. Article 25 and 26 has been problematic
      1. India does not have adequacy finding, blocks transfer data to Indiana
      2. But USA does not have an adequacy finding (see Safe Harbor agreement)
   4. Can use contracts to create legal rights where adequate data protection may not exist
      1. Ex. GE volunteered to be subject to EU data protection law in all of their global offices via k; corporation will adopt rules that implement EU law, irrespective of the non-EU nation’s legal obligations (where adequacy does not exist)
7. Applying Article 25 to the Internet: *Bodil Lindqvist* 
   1. Creates a webpage for basic information on church confirmations, and provides a description of fellow EEs at the church
      1. Descriptions include names, responsibilities, and jokes about each of them
      2. One colleague had injured her food, and was on half time leave, and this led to prosecution initiated b Swedish data prosecutor for violation of Swedish data directive (verbatim EU directive) in reference to the medical condition
   2. Publishing this medical information on the website violated data protection law in Sweden because she illegally processed personal information (did not have consent of the data subject) as well as health information
      1. Did **not violate** Article 25 exporting on data, because making information available on a **website is not considered a transfer outside the EU**
      2. Had it gone the other way, every website would have been at issue, major compliance issues
8. Article 8: Sensitive Data
   1. Certain data is considered to be so private or present such a risk that the directive has singled them out to say you cannot process this data except under certain exceptions
      1. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life
   2. Exceptions, thus such data may be processed when:
      1. Data subject explicitly consents
      2. Necessary to carry out subject’s vital interests
      3. Processing of data made public by the data subject or necessary to exercise or defend legal claims
      4. Where processing is by a health professional subject by national laws to maintain personal confidentiality
9. Safe Harbor Agreement in Response to Article 25
   1. US entity that wishes to be able to move data from the EU to the US without going through individual consent or through a derogation, signs up to be a voluntary members of the safe harbor agreement
      1. Basically just smoke and mirror approach between US and EU
   2. Utilizes the section heads of the OECD guidelines, and consenters promise to do those things, even though those guidelines in now way comply with the Directive
      1. Complying with OECD is sufficient (if US cannot comply with the Directive and you enforce it, we all lose)
      2. Enforcement mechanism is the FTC; enforces these voluntary agreements, and if you fail to follow through it is a deceptive act (violation of FTC act)
      3. To entities out of FTC jurisdiction, other departments (such as the Department of Transportation) would regulate safe harbor
      4. Entities outside any jurisdiction are left out of the safe harbor explicitly (financial corporations)
   3. Within Europe, parliaments voiced opposition, but had no say
      1. Until last year, no case filed under the safe harbor agreement
   4. For a long time no one signed up for the safe harbor
      1. But it is still a bilateral agreement between US and EU in a multi-national informational flow world
      2. However, excludes on of the largest sectors of the US economy (financial industry)
10. Problems with complying with US discovery in International Data Transfer: *VW v. Valdez* 
    1. Defendants have given them the phone book from when the car was designed and have identified all people in response to interrogatories involved in the design
       1. Argues there is no reason why a current corporate phone book of VW is necessary
    2. VW said we cannot give you the phone book because it is covered by German data protection law, hence Texas looked at the Restatement of Foreign Relations Law
       1. Under the R2d, trial court failed to balance interest of the foreign sovereign (where German privacy laws explicitly conflict with Texas discovery), with those of the real parties in any respect
       2. Trial court rejected consideration of German law, and was abuse of discretion
    3. Represents how seriously these data protection issues are taken by authorities responsible for enforcing them, German government took time to supply experts and amicus brief
       1. Issues occur in US courts every day, and considering this concerned a minimal issue (updated phone book), fights about more significant issues will be increasingly burdensome