Privacy Law - Yoo/Steinfeld Spring 2019

Alex Mueller

# Government Surveillance

## Constitutionality of Government Surveillance Methods

* Two steps to the legal analysis
  1. Compliance with constitutional restrictions
  2. Congressional authorization under constitutional authority
* This section is concerned with the former, specifically 4th Amendment constitutionality
* **4th Amendment**
  + The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized
  + Does it give basis for searching private property?
    - It is prohibitive in nature, so does not do so affirmatively. The word privacy never appears in the Constitution! – so the right to privacy is a bit constructed
    - Almost no authorizations of constitution are self-enforcing, instead they merely provide boundaries and invitations for congress to act
      * Constitutionality then becomes a matter of statutory analysis
  + Why is 4th Amendment relevant here?
    - Privacy is implicated in unreasonable searches and seizures
    - 4th Amendment violations remedied through the exclusionary rule
      * Effective at creating incentives to comply with 4A
      * Comes at price of absolving parties that are clearly guilty of an offense
  + Why are there more restrictions on government intrusions than on private entities?
    - Government is unique insofar as it has a monopoly over the exercise of power
* **Reasonable Expectation of Privacy Test:**
  + A "search" occurs for purposes of the Fourth Amendment when the Government violates a person's "reasonable expectation of privacy." - Harlan in Katz
  + Later becomes two-prong test:
    - Governmental action must contravene an individual's actual, subjective expectation of privacy
    - Expectation of privacy must be reasonable, in the sense that society in general would recognize it as such
  + Considerations:
    - To what extent is "reasonable expectation" question a normative one rather than a positive one?
    - Alito in *Jones*: Functional analysis examining qualitative factors (e.g. duration, nature of information, etc)
  + Problems
    - Susceptible to societal change
    - Standard rather than a rule – easier to apply, harder for individuals to know when their privacy is protected
    - Conditioned expectations – all the government has to do is announce that it's going to start recording all phone calls and then the reasonable expectation of privacy is gone. Government can move needle
    - Polls indicate that things SCOTUS has ruled don't have a reasonable expectation of privacy are in fact viewed as highly intrusive by Americans (drug dogs, bank records)
* **Plain view doctrine**
  + If something is in the plain view of a police officer, then he doesn't need a warrant to seize it → if something can be seen/heard from a public vantage point, then it doesn't get 4th Amendment protection. (how far does this go? Are telescopes/super-powerful microphones allowed?)
* **Third-party doctrine**:
  + You have no reasonable expectation of privacy with regard to any information you share with a third party
  + Critiques
    - Sharing info with a specific person or class of persons is not broadcasting it for the world to see
    - Content/non-content distinction is often hazy
    - Often lack of meaningful alternatives to activities involving disclosure to 3rd parties
    - Disconnect between application and people's beliefs
* **Open fields doctrine**
  + Established in *Oliver v. US* - No reasonable expectation of privacy in your private fields (despite no trespassing signs)
  + Curtilage – Parts of one's property immediately outside one's home don't fall under this rule and are subject to the usual reasonable expectation of privacy test
* Other Considerations
  + Who Should protect privacy?
    - Congress: can act ex ante and control own agenda; democratically elected
    - Courts: ex post; people can't dance around the law

## 4th Amendment Cases

### *Olmstead v. United States* (1928)

* Communications intercepted by tapping into telephone lines
* Majority holds this did not violate 4th Amendment protection of information obtained by physically intruding on a constitutionally protected area
  + Based on historical purpose of 4th Amendment, which was to prevent exercise of government force to search person, their house, or their effects against their will
  + Since there was no physical entry into the home or offices of the suspect, there was no unlawful search under 4A
  + Recites "trespass doctrine", which was exclusive controlling standard until *Katz*
* Brandeis Dissent
  + As technology advances, court must adapt in order to protect privacy interest. This surveillance method is not qualitatively different that intercepting mail, which court has held violates 4A
* \*Notes cases:
  + *Lewis v. US/Hoffa v. US* – Undercover agents who talked with defendants are constitutionally allowed to offer evidence against the defendant.
    - If the home were such a sacred area, then defendant's consent wouldn't be able to waive his privacy interest there
  + *On Lee v. US* – using a hidden microphone (strapped to an undercover officer) to gather evidence against the defendant is constitutional
  + *Silverman v. US* – police use spike mic to spy on the defendant, ruled unconstitutional because the spike mic trespassed on the defendant's private property

### *Katz v. United States* (1967)

* Facts: Wiretap placed on exterior of public phone booth without a warrant
* Holding:
  + Court rules that *Katz* was justified in expecting the contents of his call to be private, thus protected under 4th Amendment" when entering the booth and shutting the door
  + Introduces the "**reasonable expectation of privacy**" standard
    - Departure from the "trespass doctrine" which prohibited methods whereby government obtains information by physically intruding on a constitutionally protected area. Appears to displace this doctrine?
    - "**Fourth Amendment protects people, rather than places**"
    - Governs not only the seizure of tangible items, but extends as well to the recording of oral statements

### *United States v. White* (1971)

* Background: "Misplaced trust" case where police obtained oral evidence by attaching wire to cooperating confidante of suspect. The government agents overheard these conversations through a wire-tap the informant was wearing
* Holding:
  + Court holds that there is no interest in case protected by 4th amendment, as it offers no protection to mistaken belief that a person who one voluntarily confides in won't reveal information
  + "However strongly a defendant may trust an apparent colleague, his expectations...are not protected by the Fourth Amendment"
  + Pointing to case involving disclosure to undercover police agent, court similarly holds that recording by person acting on behalf of police does not constitute a search
* Dissent (Douglas, J.): Electronic surveillance is the modern means of eavesdropping; it is an assault on privacy and therefore should be regulated by 4th Amendment protections
* Dissent (Harlan, J.): The immediate relaying of info to government agents via electronic surveillance should be protected under 4th Amendment and a warrant should be required

### *Smith v. Maryland* (1979)

* Facts: Pen register case challenged on 4th Amendment grounds. Police arrest D based on information obtained via pen register installed on his phone without a warrant
* Holding:
  + Rules that **a person has no legitimate expectation of privacy in information that the person voluntarily turns over to third parties**
    - Applies to phone numbers, which are voluntarily conveyed to cell-carriers a means of establishing communication
    - Pen register did no constitute a search - privacy of what is said on the call is not infringed by this technique
      * **Content/non-content distinction**
    - Defendant “assumed the risk” that the company’s records “would be divulged to police.”
* Marshall Dissent - Privacy is not a discrete commodity. Such voluntary disclosures to a third party does not mean people have assumed the risk that the information will be passed on to the police. People have no practical alternative to using a telephone, so it's absurd to tell people they need to assume the risk of disclosure. Also, pen registers could be used by the government to halt political dissent, so their use should be regulated by warrants
* Stewart Dissent - Revealing who a person speaks with on the phone actually reveals intimate details about his or her life.There was a reasonable expectation of privacy here

### *Kyllo v. United States* (2001)

* Facts: Federal agents used thermal imaging device aimed at home to detect illegal activity occurring on the inside. Challenged on 4th Amendment grounds
* Holding:
  + Court holds that **where government uses advanced technology to explore details inside the home that would have previously been unknowable without physical intrusion, the surveillance is a search and a warrant must be obtained**
    - Permitting this method would put homeowners at the mercy of advancing technology
    - Court has held for nearly a century that 4th Amendment draws firm line at entrance to house, thus to draw another arbitrary line for details that are not "intimate" would be both unpractical and a violation of that principle. Protections shouldn't be tied to the degree of intrusions into the home
* Dissent (Stevens): Heat from the home had entered the public domain and the police's observation of it was not a search. Plain view doctrine should apply here
* *CA v. Ciraolo* (Notes) – Police don't have to shield their eyes when driving past homes
  + Scalia thinks Katz imposed a requirement on top of that imposed in Olmstead rather than overruling it

### *United States v. Forrester* (2008)

* Background: Challenges to validity of surveillance mechanism, by which government monitored volume/destination of emails and web traffic, under the 4th amendment
* Holding:
  + Court cites both *Katz* (that expectation of privacy extends to the contents of a phone call) and *Smith* (that phone call metadata, rather than the contents, are captured using pen register and thus there is no violation)
  + Court finds this case analogous to *Smith* in that **there is no reasonable expectation of privacy for destination IP addresses when relying on 3rd party equipment to communicate** (i.e. route the traffic)
    - Like in *Smith*, the **contents of the communication are not revealed. Thus, court ruled method did not constitute a 4th amendment search**

### *United States v. Warshak* (2010)

* Facts: Government suspects Warshak of defrauding customers, so requests ISP preserve contents of emails and provide them without warrant
* Holding:
  + Court holds that **reasonable expectation of privacy extends to content of emails stored with or sent/received through a commercial ISP, as it does to contents of communication over other mediums**
    - **Government may not compel an ISP to turn over the contents of a subscriber’s emails without a warrant**
    - ISP is the functional equivalent of post office or phone company, neither of which can be compelled to reveal contents of customer communications without a warrant

### *United States v. Jones* (2012)

* Facts: FBI attaches GPS on suspects truck to track movements after warrant had expired
* Holding: Plurality finds that this violated 4th Amendment protections against unlawful searches
* Scalia Opinion - A vehicle is an “effect” for Fourth Amendment purposes. Thus, the government’s installation of a GPS device on Jones’s vehicle constitutes a “search.” While acknowledging *Katz* still applies in cases involving communication signals where there is no trespass, the trespass here was clear and thus is the basis for the search's unlawfulness
  + Returns to formalistic property based standard, while acknowledging *Katz* still exists
* Concurrence (Sotomayor): Physical intrusion isn't the only way that the government can violate your privacy. Search is defined by the type of information take. Writes that *Smith* decision should be reconsidered to better suit digital age, however, Physical intrusion provides narrower basis for decision
* Alito Concurring in Judgement - Argues against application of trespass doctrine post-*Katz*. Invites legislative action to regulate these methods, but until then, the reasonable expectation test in *Katz* should apply. Majority fails to address the possibility that the government could violate your privacy without physical intrusion. The length/invasiveness of the tracking is the crucial factor
* Shadow Majority - Sotomayor joins Scalia majority despite appearing to adopt reasoning of Alito. This underscores need for additional clarity

### *Riley v. California* (2014)

* Facts: Police searched D incident to an arrest and seized his smartphone. The police searched the smartphone and used items found as evidence at D's trial on shooting charges brought by CA. D was convicted. On appeal, the court determined the warrantless search was a valid search incident to arrest
* Holding: Under 4th Amendment, the **government may not conduct a warrantless search of the contents of a cell phone seized incident to an arrest absent exigent circumstances**
  + Absent more precise guidelines, court generally determines whether to exempt search from warrant requirement by **assessing degree to which it intrudes privacy against the degree to which it is needed to protect government interests**
  + Searches incident to arrest are allowed only to ensure officer safety or to prevent the destruction of evidence. The interest in preserving evidence can be served by confiscating the phone and then waiting for a warrant to search it (you can put it in a black box if you really have to). Police can get more info from searching the phone than from searching an entire house.
    - Mosaic Theory – Allowing police to view which apps you use through the third party doctrine would allow them to make a complete picture of you
  + Concurrence (Alito): State legislatures are better suited to address this issue through new laws than federal courts are through 4th Amendment decisions

### *Carpenter v. United States* (2018)

* Background: Case where cell-site location information, which reveals location of phone based on nearest cell-tower, was obtained from carrier and used to convict suspect for involvement in robbery
* Holdings:
  + Court declines to extend "third party" principle articulated in *Smith*, in which there is no reasonable expectation of privacy when information is voluntarily divulged with 3rd party, to the present circumstances
    - As technology advances, court acknowledges need to preserve degree of privacy 4th amendment intended to protect at time of adoption. It could not be foreseen, at time of *Smith*, a world in which phones are capable of tracking owners movements
  + Thus, **using CSLI to record an individual's movements over period of time constituted a search**. Individual maintains a legitimate expectation of privacy
* Majority Reasoning
  + CSLI does not “fit neatly under existing precedents,” and that it instead lies at the “intersection of two lines of cases” the first line addressing geolocation, and the second addressing the third-party doctrine
    - Geolocation
      * Roberts quotes Justice Alito’s *Jones* concurrence, noting that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"
      * "Even greater privacy concerns than the GPS monitoring of a vehicle we considered in Jones," because a cell phone is almost a "feature of human anatomy" (quoting Riley) and "tracks nearly exactly the movements of its owner"
    - Third Party Doctrine
      * The services carriers provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society, thus cell phone location information is not truly ‘shared’ as one normally understands the term,
      * Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily “assume[] the risk” of turning over a comprehensive dossier of his physical movements
    - There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today
  + Conclusion: "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection," writing that "the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."
* Dissent
  + Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. Cell-site records are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process
    - This principle established in Miller and Smith should control
    - The defendants in those cases could expect that the third-party businesses could use the records the companies collected, stored, and classified as their own for any number of business and commercial purposes. The businesses were not bailee's or custodians of the records, with a duty to hold the records for the defendants’ use. The defendants could make no argument that the records were their own papers or effects
  + That line that the majority draws illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations
* Problems with Carpenter:
  + Creates even more uncertainty. Suggestions of a narrow ruling, meaning *Smith* 3rd party doctrine is still good law. Essentially a balancing act between privacy interests and disclosure
  + Balancing test might compromise away rights due to the immediacy of concerns which compel disclosure

### Workplace and Hotel Searches

* Work Issued Pagers (Notes)
  + Facts: Ontario, CA issued pagers to its police officers. Employees went over the word limit, sending personal messages and causing the city fees. The city obtained transcripts of the texts, which the officers argued was a violation of their 4th Amendment Rights
  + Holding: Regardless of whether officers had a right to privacy on the pagers, the **search was constitutional because it was motivated by a legitimate work-related purpose, and not excessive in scope** (consistent with the court’s prior ruling in *O’Conor v. Ortega*)
    - Emphasized past decisions holding “operation realities” can reduce an employee’s privacy expectations and that these can be taken into account when considering if a workplace search is constitutional

## Overview of Surveillance-limiting Statutes

* Historic Statutes
  + Section 605 of the Federal Communications Act of 1934 – nation’s first major anti-wiretapping statute
    - Provided that “No Person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance… of such intercepted communication to any person”
    - Did not prevent use of wiretaps – just restricted admissibility of evidence gained via wiretap into court
  + Title III of the Omnibus Crime Control and Safe Streets Act of 1968 – Nation’s second major statute limiting surveillance goes much further
    - Enacted same year as *Katz* (which recognized right to privacy in telephone communications) and *Berger v. New York* (found a state statute that regulated scope of electronic surveillance didn’t adequately protect 4th Amendment rights)
    - Attempted to establish strong privacy safeguards, recognizing also legitimate circumstances that may require use of surveillance
    - Regulated both face-to-face communications and telephone calls
    - Supplanted by the Electronic Communications Privacy Act
* **Foreign Intelligence Surveillance Act of 1978** – passed to address special demands of national security and foreign espionage left open by *Katz*
  + Established a procedure through which government agencies could obtain expedited, top-secret approval for national security-related surveillance
* **Electronic Communications Privacy Act of 1986**
  + Addressed major developments in technology, such as the growth of email
  + Sought to overturn decision in *Smith v. Maryland* (third-party doctrine)
  + ECPA has been amended many times
  + Often referred to as Title III as it was technically an amendment to Title III of the Omnibus Crime Control Act (Wiretap Statutes)
  + **Title I of ECPA – (Wireless and Electronic Communication Interception Act (“Wiretap Act”)**
    - Prohibits intercepting oral, wire, or electronic communications during their transmission
    - Covers landlines, cell phones, satellite communications, and emails in flight and in "transient storage" during transmission
  + **Title II of ECPA – Stored Wire and Electronic Communications Act (“Stored Communications Act”)**
    - Makes it a crime to obtain, alter, or block access to a wire or electronic communication in electronic storage
    - Governs access to stored email and voice mail
    - Also governs ISP’s ability to provide 3rd party access to user and subscriber data
  + **Title III of ECPA – Pen Register Act**
    - Regulates use of pen registers and capture of non-content portions of wire and electronic communications
    - Regulates called ID equipment and other “trap and trace” devices that capture outgoing/incoming phone numbers
* Digital Telephony Act of 1994 (“Communications Assistance for Law Enforcement Act,” “CALEA”)
  + Amended ECPA - Reflected concerns that emerging technologies would frustrate law enforcement surveillance
  + Requires telecommunication providers to modify their equipment, facilities, and services to ensure they have the necessary surveillance capabilities
  + Extended ECPA Title I to cordless phones (which were previously excluded based on their radio technology)
* **USA PATRIOT Act** - a.k.a Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
  + Aimed at facilitating the global war on terrorism, including domestic terrorism
  + Temporarily shifted stored wired communications from Wiretap Act to SCA, which has lower standard of approval and no exclusionary rule
  + Authorizes SCA warrants to be nationwide. Court can delay notice of search warrants if it concludes that there is reasonable cause that immediate notice will create an adverse result
* Cyber Security Enhancement Act of Homeland Security Act of 2002
  + Amended ECPA Title II to battle computer crimes and release ISP from liability for good faith disclosures to government of customer info in electronic storage
  + ECPA does not regulate video-only surveillance nor provide clear guidance on GPS or cell phone tower-based positioning data gathering
* USA Freedom Act
  + Ended bulk collection of telephone toll records

## ECPA Title I (Wiretap Act) and its Predecessor (Omnibus Crime Control - Title III)

* With Title III, Congress sought to regulate use of electronic surveillance as an investigative tool and disclosure of materials obtained through surveillance
* Purpose is to control conditions under which interception will be permitted to safeguard privacy of wire and oral communications
  + “Animating Title III is an overriding congressional concern with the protection of individual privacy”
  + Surveillance techniques are authorized only in investigations of serious offenses, is all subject to prior judicial approval which is issued in accordance to detailed application procedures and finding of probable cause
* Most clearly reflected in Title III’s strictly limited disclosure provisions, permitting disclosure of intercepted communications in 3 circumstances only:
  1. Law enforcement may disclose to another law enforcement officer to the extent required to perform duties
  2. Law enforcement can use the contents to extent appropriate to perform their duties
  3. While giving testimony under oath
* Explicitly authorizes recovery of civil damages by persons whose communications are disclosed in violation of the statute
* Richard Turkington: analysis of ECPA Title I (“Title III”) cases
  + 4 steps analysis should be utilized in evaluating Title I cases:
    1. Determine if there was an interception of a communication
    2. Determine whether there is a section 2517 exception
    3. Determine if interception satisfies section 2518 (which establishes the necessary procedure for obtaining court ordered electronic surveillance
    4. Consider applicability of a criminal sanction, civil remedy, or right to exclude

### Wiretap Act

* Only when normal methods of investigation are infeasible
* Three types of communications:
  1. Wire communication – aural transfer made by wire
  2. Oral communication – utterance by a person
  3. Electronic communication – transfer of signals by wire or spectrum that is not wire or oral communications
* **18 U.S. Code § 2510 - Definitions**
  + **Electronic communication** - any transfer of signs, signals…of any nature by a wire, radio, electromagnetic…system that affects interstate or foreign commerce, but does not include:
    - Any wire/oral communication
    - Tone-only paging devices
    - Tracking devices
    - Electronic funds transfer information
  + **Wire communication** - any aural transfer made…by the aid of wire, cable, or other like connection…furnished or operated by any person engaged in providing…such facilities for the transmission of interstate or foreign communications…and such term includes any electronic storage of such communication
  + Other definitions:
    - “**Aural transfer**” means a transfer containing the human voice at any point between and including the point of origin and the point of reception
    - “**Intercept**” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device
    - “**Electronic, mechanical, or other device**” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business
    - "**Readily Accessible to the General Public**” - means, with respect to a radio communication, that such communication is not—(A) scrambled or encrypted; (B) transmitted using modulation techniques that preserve the privacy of such communication;(C) carried on a subcarrier or other signal subsidiary to a radio transmission; (D) transmitted over a communication system provided by a common carrier, unless a tone only paging system
* **18 U.S.C §2511 - Interception and disclosure of wire, oral, or electronic communications prohibited**
  + §2511(1)
    - Except as otherwise specifically provided in this chapter any person who
      * (a) intentionally intercepts…any wire, oral, or electronic communication;
      * (b) intentionally uses…any electronic, mechanical, or other device to intercept any oral communication…
  + Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)
  + §2511(2)
    - (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person-
      * (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public
    - (ii) to intercept any radio communication transmitted: (I) for the use of the general public or relates to ships, aircraft, vehicles, or persons in distress, (II) governmental, law enforcement, civil defense, private land mobile, or public safety readily accessible to the public, (III) ham or CB, (IV) marine or aeronautical
* Wiretap Act has highest standard and strongest privacy protection of the 3 main ECPA provisions
  + Not only requires law enforcement **have probable cause to believe intercepting phone calls will lead to evidence of specific, enumerated crimes** (i.e. those listed in §2516), but also requires law enforcement to demonstrate:
    - **(1)** Probable cause that communications regarding the crime will be obtained by the wiretap (§2518(3)(b))
    - **(2)** Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous (§2518(3)(c))
    - **(3)** Probable cause to believe the phone number or other electronic “facility” where the communication to be intercepted occurs has a connection to the crime or person to be wiretapped
  + Also imposes requirements to ensure surveillance does not exceed that which is reasonably necessary (§2518(5)):
    - No order entered under this section may authorize or approve the interception...for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days
    - Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days
* Application of Wiretap Act to Email
  + Electronic communications includes communications in transient storage intrinsic to communications process
  + Email not yet read is subject to the Wiretap Act
  + Email in pre- and post-transmission storage is governed by the SCA
* Application of Wiretap Act to Wi-Fi
  + Capturing payload data violates Wiretap Act
  + “Readily accessible the general public” applies only to “radio communication” like traditional radio (i.e. auditory broadcasted communications)

### Minimization Requirement - *Scott v. United States* (US Supreme Court – 1978)

* Facts: Title III requires wiretapping or electronic surveillance "be conducted in a way as to minimize" interception of communications not otherwise subject to interception under Title 18 § 2518(5). Government got wiretap approval and agents intercepted for one month virtually all conversations of suspects. 40% of the calls were clearly narcotics related, and the remaining calls were for the most part short. D argues there was no good-faith effort to comply with minimization requirement, in violation of statute.
* Holding (Rehnquist):
  + Proper approach for evaluating compliance with the minimization requirement, like evaluation of all alleged violations of 4th Amendment, is **objectively to assess the agent's or officer's actions in light of the facts and circumstances confronting him at the time, without regard to his underlying intent or motive**
  + Even if agents fail to make good faith efforts at minimization, that is not itself a violation of the statute requiring suppression, since use of the word "conducted" in §2518(5) makes clear the focus was to be on the agents' actions, not motives
  + Whether the way in which a wiretap was conducted is reasonable will depend on facts and circumstances of each case
    - % of non-pertinent calls intercepted not a sure guide to correct answer; also important to consider the circumstances of the wiretap (could be ambiguous or used coded/guarded language)
    - **Short and ambiguous nature of non-pertinent phone calls did not give the agents an opportunity to develop a category that should not have been intercepted, and hence their interception cannot be viewed as a violation of the minimization requirement**
* Dissent (Brennan): The minimization requirement was central to passage of Title III and the court is disregarding this in their majority decisions, as the minimization requirement was clearly violated by the agents

### Intercepting Emails In-Flight/Transient Storage: *United States v. Councilman* (1st Circuit – 2005)

* Facts: Interloc gave book dealer customers an e-mail address at the domain "interloc.com" and acted as the e-mail provider. CEO ordered employees to configure mail server to copy all incoming communications to subscriber dealers from Amazon.com (competitor). D contends the email messages were not “electronic communications” and the method they were copied was not “interception” under the Wiretap Act
* Issue - one of statutory construction
* Holding: 1st Circuit reviewed and holds that D's interpretations ere inconsistent with congresses intent
  + D infers that Congress intended to exclude communications in transient storage from the definition of "electronic communication" regardless if still in the process of reaching end destination, simply because it was not specifically enumerated in the statute
  + ECPA text does not suggest whether or not electronic storage while in transmission falls under Wiretap Act. Court thus turns to legislative history, which it determines establishes that **electronic communication includes transient storage intrinsic to the communications process. Thus, the conduct in this case violated the Wiretap Act as copying this communication constitutes and "interception"**
* EPIC Amicus Brief
  + Internet-based mail services clearly distinguish between the routine storage that occurs when a message reaches its destination and is available to its intended recipient and the temporary “storage” that occurs as electronic mail moves in many discrete steps from sender to recipient
  + "Storage” occurs only at the endpoint when a message is accessible to the intended recipient
  + Access to an Internet communication before it was accessible to the intended recipient would be considered an “interception

### Intercepting Wifi Communications - Joffe v. Google Inc. (9th Circuit Court of Appeals – 2013)

* Facts: While capturing Street View photos, Google collected data from unencrypted Wi-Fi networks (“payload data”). Google was sued under Wiretap Act
* Holding:
  + Wiretap Act exempts intercepting “electronic communications made through an electronic communication system” if the system is configured so that it is readily accessible to the general public (radio communication also exempted) – so Google argued its collections were exempted
  + Court agrees with Google that the definition of “readily accessible to the general public” apples to the §2511 exemption, when the communication in question is a radio communication
  + However the **“radio communication” in § 2510 excludes payload data and the court chooses to adopt the “common meaning” of the phrase “radio communication” (which is commonly understood to be “1) predominantly auditory and 2) broadcast”).** Therefore the data collected by Google is a violation of the Wiretap Act
  + If Congress has intended satellite to be encompassed in a “radio communication,” they wouldn’t have called it out separately. Thus, can't assume radio communications extends to things like satellite television

## ECPA Title II - Stored Communications Act

* **§2701 – Unlawful access to stored communications**
  + **§2701(a) - Offense**
    - Except as provided in subsection (c) of this section whoever—
      * (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
      * (2) intentionally exceeds an authorization to access that facility;
    - and thereby obtains, alters, or prevents authorized access to a wire or electronic communication **while it is in electronic storage** in such system shall be punished as provided in subsection (b) of this section
  + **§2701(c) - Exceptions**
    - Subsection (a) of this section does not apply with respect to conduct authorized:
      * (1) by the person or entity providing a wire or electronic communications service;
      * (2) by a user of that service with respect to a communication of or intended for that user; or
      * (3) in section 2703, 2704 or 2518 of this title
* **§2702 - Voluntary Disclosure of Customer Communications or Records**
  + **§2702(a) - Prohibitions**
    - Except as provided in (b) or (c)—
      * (1) a person providing an electronic communication service shall not knowingly divulge the contents of a communication while in electronic storage by that service; and
      * (2) a person providing remote computing service (storage or computer processing) shall not knowingly divulge the contents of any communication which is carried on that service from and for those subscribe for the sole purpose of storage and processing services
      * (3) a provider of remote computing service or electronic communication service shall not knowingly divulge a record pertaining to a subscriber to or customer of such service
* **§2703 - Required Disclosure of Customer Communications or Records**
  + **§2703(a) - Contents of Wire or Electronic Communications in Electronic Storage**
    - A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section
  + **§2703(b) - Contents of Wire or Electronic Communications in a Remote Computing Service**
  + (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication
    - (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant
    - (B) with prior notice to the subscriber if the governmental entity
      * (i) uses an administrative subpoena authorized by statute [no judicial oversight] or
      * (ii) obtains a court order for such disclosure under subsection (d)
* **§2510(17) - Definition of "Electronic Storage":**
  + (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
  + (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication
* **§2510(15) – Definition of “Electronic Communications Service”**
  + Any service which provides to users thereof the ability to send or receive wire or electronic communications
* **§2711(2) – Definition of “Remote Computing Service”**
  + The provision to the public of computer storage or processing services by means of an electronic communications system

### Access to Stored Email - *Jennings v. Jennings* (Court of Appeals of South Carolina – 2012)

* Facts: Woman discovered card in husbands car for flowers and confronted him. Husband was having an affair with a woman he corresponded with at work. Woman’s daughter-in-law, "hacked" (really just guessed password) husband’s web based email account to find out who the other woman was. Husband sues under the SCA
* Rules:
  + Under §2701, a violation of the SCA occurs by anyone who:
    1. Intentionally accesses without authorization a facility through which electronic communication is provided, or
    2. Intentionally exceeds authorization to access that facility
  + SCA defines electronic storage as:
    - A) Temporary, intermediate storage of a ware or electronic communication incidental to the electronic transmission and
    - B) Any storage of which such communication by an electronic communication services for the purpose of backup protection
  + **Thus, SCA only pertains to communications intercepted or accessed prior to delivery to the intended recipient or in backup storage**
* Holding:
  + D not liable under the SCA, as the emails were not in “electronic storage” (as they were on the Yahoo! Server and apparently were not retained in such as way as to qualify as “backup protection” as required by the statute)
    - Court declines to extend backup protection under statute to the act of simply retaining opened emails on the server, which is what happens by default in the absence of any additional actions (e.g. deleting from server)
      * Backup necessarily presupposes the existence of another copy to serve as a substitute. No reason to deviate from this meaning
* Concurrence : Traditional interpretation of the SCA (e.g., the DOJ’s interpretation is the correct version); the majority relies on Weaver; advocates that “electronic storage refers only to 1) temporary storage made in the course of transmission and to 2) backups of such intermediate communications. This rejects the local/cloud distinction from *Theofel*, meaning final destination is reached upon being opened
* Notes:
  + SCA creates criminal liability and expressly provides for private right of action against violators
  + It was the express intent of Congress in enacting the SCA to bar anyone from accessing communications without permission and to bar providers of electronic communication services from knowingly diverging
  + The *Jennings* decision was met with sharp criticism
  + **The most followed interpretation of what it means to be in “electronic storage” is from the 9th circuit in, holding “prior access is irrelevant to whether an email is in electronic storage”**

### ISP Liability for Police Disclosures - *Freedman v. America Online Inc.* (D. Conn – 2004)

* Facts - D1, police officers, sent an improper search warrant (no judge signature) to AOL (D2) who sent back P's information. P sued under the Electronic Communication Privacy Act, arguing that soliciting information disclosure by AOL with invalid search warrant violated ECPA as did AOL's compliance with the request
* Holding: Movement for partial summary judgement was granted to extent that finds D1 in violation of the ECPA
  + ECPA distinguishes between rights of government entities and rights of private entities regarding discloser of subscriber info by an ISP. Governmental entity must comply with specific legal process (e.g., a search warrant, subscriber consent, etc.)
    - Holding here relies on McVeigh v. Cohen, holding government is liable for soliciting subscriber info without complying with ECPA’s legal process requirements
  + Defendants argue they didn’t require AOL to disclose – court finds this argument “disingenuous” and doesn’t absolve them from liability. It also contradicts Congress' intent to protect personal privacy. ECPA imposes obligation for ISP to comply and the request resembled compulsory court order, thus reasonably likely that AOL simply thought they were complying. AOL was clearly expected to respond here, and this erodes congressional intent
  + Defendants also contend there is genuine dispute of material fact on whether the emergency exception applies – Court rejects this, as no “immediate danger” and no evidence about what AOL may have actually believed was provided

### Email Acquisition via Overbroad Subpoena - *Theofel v. Farey-Jones* (9th Circuit – 2004)

* Facts: Civil matter in which an ISP handed over hundreds of private emails during course of discovery in response to a request for all emails (rather than a limited scope of emails)
* Holding: **Emails delivered, read, and on an ISP server are still electronic storage for purposes of the SCA**
  + Court reject D's first argument that access was authorized because ISP turned over emails in response to subpoena
    - SCA reflects Congress' judgement that users have a legitimate interest in the confidentiality of communications in electronic storage, similar to common law trespass protections
    - Federal statutes are interpreted in light of common law – which court finds implies “**no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access**”
    - Defendants clearly knew the subpoena was invalid, as it was so outrageous, and its immaterial that NetGate could have objected as the subpoena was deceptive and that is an independent ground for violating consent
  + Court also rejects defense that messages were not in stored communication thus there is no violation of the SCA
    - Since read/delivered emails are no longer in transmission, primary issue becomes whether their storage is for the purpose of "backup
    - An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again — if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition
    - **SCA Subsection B “by its plain terms, applies to backup storage regardless of whether it is immediate or post-transmission”**
    - The US Government, as amicus curiae, disputed the court’s interpretation, stating subsection (b) refers only to backup copies of messages that are in of themselves temporary (as this would make accessing emails such as these more difficult). Court rejects this interpretation, saying their is no reference to subsection (a), thus no reason to infer that "temporary" storage language should factor into subsection (b)
    - Court also rejects argument that its interpretation renders meaningless the separate (and more liberal) standard for remote computing services. Message stored by RCS (cloud) would not necessarily be stored for purposes of backup protection and thus subject to more stringent standards set forth in §2703(a). This is significant because **an RCS (cloud) might be the only place a user stores his messages, thus the messages are not stored for backup purposes in these cases**
* Outcome: Reverse dismissal of the Stored Communications Act claim, affirm dismissal of the Wiretap claim (holding this act only applies to interception contemporaneous with transmission, not while in electronic storage), and reverse dismissal of the Computer Fraud and Abuse Act claim
* Notes:
  + In re National Security Agency Telecommunications: neither FISA, ECPA Title II, nor federal common law completely preempts state law for greater privacy protection
  + In this case, petition to remand to state court was still denied because US government intervened as plaintiffs, making the case removable on other grounds

### Who is an “Electronic Communication Service” under Title II? – The Airline Passenger Data System Exclusion

* *Dyer v. Northwest Airlines Corp.* (D.N.D. – 2004)
  + Facts: Post-9/11, NASA requested system-wide passenger data from Northwest airlines for a 3-month period, and Northwest complied. This triggered a wave of litigation
  + Holding: “Electronic communication service” encompasses ISPs and telecommunication companies – but does not encompass businesses selling products online – so, Northwest is not an ISP and outside the scope of §2702 and the ECPA as a matter of law
* *In re JetBlue Airways Corp. Privacy Litigation* (E.D.N.Y. – 2005)
  + Facts: JetBlue maintains “Passenger Name Records” on each of its passengers, In creating the PNRs, JetBlue’s privacy policy said it would not share customer financial data with 3rd parties. Post-9/11, TSA got involved and requested the data from JetBlue, who agreed to cooperate. In 2003, JetBlue CEO disclosed this, leading to a series of suits under ECPA, among other statutes. JetBlue filed Rule 12(b)(6) motion
  + Holding: JetBlue is **not an electronic communication service provider as a matter of law within the meaning of ECPA nor a remote computing service, thus it is not liable under §2702 of ECPA**

### National Security Letters (NSLs) and the "Gag" Requirement - *Doe v. Gonzales* (2d Cir. 2006)

* Background:
  + National Security Letters (NSLs) - Administrative subpoenas use to gain access to subscriber info and billing record from providers of a wire or electronic communication service (e.g. an ISP) when this information is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. It was originally enforced along with a strict gag order that prohibited the recipient from disclosing the letter from **anyone**
    - Later amendments to §2709(c) permit exceptions to gag order, allowing disclosure to legal counsel, those necessary to comply with request, and other approved parties
    - Amendments also provided availability of prompt judicial review
    - Restrictions on disclosure (1A implications) and relaxed standards of approval have made these subject to much controversy
* Facts:
  + §2709 imposed a gag order on the recipients so they could neither inform anyone of receiving an NSL, nor act as witnesses
  + In 2005, Congress passed the USA PATRIOT Improvement and Reauthorization, which dramatically altered §2709
    - E.g., Revised §2709 allows an NSL recipient to talk with an attorney
  + John Doe (P) was the recipient of an NSL that requested all information associated with one of his Connecticut library’s computers
    - P argues that despite revisions to §2709, gag order is still unconstitutional and violates 1A rights
* Holding:
  + Court found non-disclosure (“gag”) rules of §2709 which prevented P from revealing identity as an NSL recipient to be unconstitutional, based on the First Amendment. It thus granted preliminary injunction because of “irreparable harm" from suppression of its speech
* Concurrence:
  + Agrees with majority, but writes separately to emphasize the need to “resolve tension between government’s interest in maintaining the integrity of its investigative process and the First Amendment” (asserts government is going beyond democratic principles)
  + Permanent ban on disclosure seems so extreme that it is highly unlikely to be justified by a compelling government interest
* Note: National Security Letter Library Exception
  + Librarians objected to the “loss of confidentiality” imposed as result of section 2709, resulting in the “Privacy Protection for Library Patrons” exclusion
  + This exclusion states that libraries will NOT be considered a “wire or electronic communication service provider” as the library’s ISP is the actual “provider” of wire service

## USA PATRIOT Act

### Susan N. Herman - Discussion of the most controversial surveillance provisions of the Patriot Act

* Section 215: Librarians and Beyond
  + Authorizes the government to acquire records and tangible things from custodians – including educational or financial institutions
  + Eliminated the requirement that government demonstrate any form of individualized suspicion
    - Merely requires FBI director or designee to certify that they believe information relevant to national security investigation
  + Contains a broad gag order that prohibits any person from disclosure to anyone “other than those persons necessary to produce those tangible items
    - Criticisms of gag order include:
      * Violates Fourth Amendment by not requiring a couple to find individualized suspicion before issuing the order and by not providing for notice to the target, even after the fact
      * Violates First Amendment, as allows gathering info about individual’s reading habits, internet activities, religious practices, etc.
    - Government responds by arguing section 215 provides more process than constitutionally required (e.g., targets have no Fourth Amendment rights)
  + *Muslim Community Association of Ann Arbor v. Ashcroft*
    - Ps believed they had been targeted under a 215 search. This potential misuse affected the behavior of community members, who became afraid to practice religion or make political expressions. However, because of the secrecy surrounding implementation of Section 215, the government has a considerable advantage in the litigation (as the Attorney General could control when and what info was divulged). Lead to difficulty establishing standing and ripeness. Proceedings took place ex parte without equal access to the facts
* Section 505: National Security Letters
  + Goes even further than 215 in circumventing judicial oversight of government collection of info from 3rd party custodians by allowing the government to obtain records from a communications provider by issuing its own administrative subpoena, called a “National Security Letter”
  + Similar to 215, no requirement for individualized suspicion and includes a broad gag rule – but criticism is even more fervent as no judicial role is contemplated at all
  + Attempt to litigate constitutionality of Section 505 - same distortions of litigation process as above
    - One brought by ISP who was served with an NSL and claimed 505 violated 1st, 4th, and 5th Amendments
    - Government argued 505 constitutional by construing it to allow the NSL to consult with counsel and bring judicial proceeding contesting constitutionality – court rejected this argument
    - Holding: did not address whether violated 4th Amendment; held 505 could be used in a manner that infringed on 1st Amendment
* Section 218: Foreign Intelligence Surveillance (FISA)
  + Expands government’s power to use Foreign Intelligence Surveillance Act (FISA) warrants to conduct electronic surveillance by only requiring FISA court approval (rather than “normal” court) (so lower standard than “probable cause”)
    - Advocates argue FISA has many safeguards similar to those required for when electronic surveillance is used in a criminal investigation (e.g., some element of a minimization requirement)
  + SCOTUS has never ruled on constitutionality of FISA, however constitutionality of 218 has been the subject of a judicial opinion (handed down in a “highly unusual ex parte proceeding”)
  + Because of the statutory scheme and constitutional law involved with 218 are so complex, its unrealistic to expect meaningful public assessment of the changes effected by 218
* Section 213: Sneak and Peek
  + Applies in cases where the government has honored the 4th Amendment norm by obtaining a search warrant based on probable cause (allows the government to ask a court for permission to defer notifying the target that a search or a seizure has taken place)
    - Critics say 4th Amendment requires notice prior to search and that failure to notify is a denial of due process
  + There appears to have been no litigation over constitutionality of 213
  + A Gallup poll indicated strong disapproval for 213 – which led Congress during the “sunset debates” (e.g., renewal period) to add in some time limits (although these also were quite elastic)

## ECPA Title III - Pen Register Act

### Pen Register Act

* **§3121(a) - In General**
  + Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under §3123 of this title or under FISA or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies §2523
* **§3121(a) - Exception**
  + Does not apply to use of pen register or trap device by provider of service:
    - Relating to operation/maintenance/testing of service
    - Relating to protecting subscribers from abusive or fraudulent use
* **§3121(c) - Limitation**
  + A government agency authorized to install and use a pen register shall use technology reasonably available to it that restricts the recording of electronic impulses so as not to include the contents of any wire or electronic communications
* **§1327 - Definitions**
  + The term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business
  + The term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

### In the Matter of the Application of the USA (Southern District of Texas – 2006)

* Issue - This opinion addresses whether the government may obtain “post-cut-through dials digits” containing communication contents under the authority of the Pen/Trap Statute
* Background
  + “Post-cut-through dials digits” = any numbers dialed from a telephone after the call is initially setup or “cut-through” (sometimes telephone numbers, or sometime real info, e.g., bank account numbers)
    - As result of this dual capacity, post-cut-through dialed digits occupy doubtful place in federal electronic surveillance law
  + During debates of CALEA, discussed the capacity of pen registers to capture content information in the form of post-cut-through dialed digits  so CALEA amended to limit use of pen registered to use them “reasonably”
  + 1999: FCC passed the “J-standard,” creating standard technical standards including capability for “post-cut-through dialed digit extraction” (means it must generate a list of all digits entered after a call has been connected)
  + 2001: During PATRIOT Act debates, expanded Pen/Trap statute to include “all dialing, routing, addressing, or signaling information” (so extended coverage to Internet communications)
  + Opponents worried this would allow government to obtain contents of communications w/o a warrant -> led to 3 amendments:
    - (1) added phrase “shall not include the contents of any comm” to the pen register definition (Section 3127)
    - (2) same phrase added to trap and trace definition (Section 3127)
    - (3) added phrase “so as not to include the contents of any wire or electronic communications” was added to the reasonably available technology limitation (Section 3121) (anything past “1-800” was considered content)
  + **It’s undisputed that post-cut-through digits can include call content**
* Holding: Post-cut through dialed digit contents may be intercepted by law enforcement under the Wiretap Act, and collected from electronic storage under the SCA. **They are not available to law enforcement under the Pen/Trap statute**. Section 3121 is a limitation, not a license. Because the Pen/trap Statute triply forbids what the government requests, the application to acquire post-cut-through dialed digits must be denied
  + Government’s argument based on what “technology is reasonably available”. No such technology exists to discern content from non-content in the case post cut-through

## FISA

### Pre-FISA Terrorism Surveillance - *United States v. United States District Court* (1972)

* Facts: US charged 3 Ds with conspiracy to destroy government property. During pretrial, US government admitted it has used electronic surveillance and that the AG had approved the wiretaps, but no judicial approval. District court found that the surveillance was unlawful and appeals court affirmed
* Issue: Does President have power, acting through the AG, to authorize electronic surveillance in internal security matters without prior judicial approval?
  + Government argues search was lawful as reasonable exercise of president’s power, the special circumstances applicable to domestic security necessitates a further exception to the warrant requirement, and that disclosure to a magistrate of all or even a significant portion of info involved in domestic security would create danger
* Holding: affirms DC and appeals court that **judicial approval is needed for domestic surveillance**. Concerns not great enough to depart from customary requirement of judicial approval
  + Recognizing that 4th amendment is not absolute and thus it must weight basic values at stake in the case by weighing the duty of government to protect domestic security and individual right to security/privacy
    - This includes asking whether warrant requirement would unduly frustrate government protection efforts against domestic terrorism
  + Rejects government’s argument that internal security matters are too “subtle and complex” for judicial evaluation
  + Emphasizes that this holding is limited to domestic, not foreign surveillance (“foreign powers and their agents”) -> This opening led to creation of FISA

### Foreign Intelligence Surveillance Act of 1978 (FISA)

* The FISA and the FISC
  + FISA prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the US on behalf of a foreign power
  + FISA Court (FISC) incudes 7-11 judges, of whom “no fewer than 3 shall reside within 20 miles of DC”
  + FISA Court of Review created to review applications denied by FISC
* **§1805(a) - Necessary Findings**
  + Upon an application made pursuant to section 1804, the judge shall enter an ex parte order as requested...approving the electronic surveillance if he finds that:
    - (2) On the basis of the facts submitted by the applicant there is probable cause to believe that:
      * (A) The target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment
      * (B) Each of the facilities at which the electronic surveillance is directed is being used by a foreign power or an agent of a foreign power;
* **§1804(a) - Approval (Significant Purpose)**
  + Each application for an order approving electronic surveillance under this subchapter…shall include:
    - (6) a certification by an executive branch official designated by the President:
      * (B) that a significant purpose of the surveillance is to obtain foreign intelligence information
* **§1801(a) - Definition of "Foreign Power"**
  + Foreign government or any component thereof, whether or not recognized by the United States;
  + A faction of a foreign nation or nations, not substantially composed of United States persons;
  + An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
  + A group engaged in international terrorism or activities in preparation therefor;
  + A foreign-based political organization, not substantially composed of United States persons;
  + An entity that is directed and controlled by a foreign government or governments; or
  + An entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction
* **§1801(b) - Definition of "Agent of a Foreign Power"**
  + Any non-US person:
    - Who acts as an officer or employee of a foreign power
    - Who acts for a foreign power which engages in clandestine intelligence activities
    - Who engages in intl. terrorism activities (or preparations)
    - Who engages in the international proliferation of weapons of mass destruction
  + Any person (incl. U.S. person) who:
    - Engages in clandestine intelligence gathering for a foreign power that may involve criminal violations
    - Knowingly engages in sabotage or intl. terrorism
    - Knowingly enters U.S. under a false or fraudulent identity on behalf of a foreign power
* **§1801(e) - Definition of "Foreign Intelligence Information"**
  + Information that relates to the ability of the United States to protect against:
    - Actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
    - Sabotage, intl. terrorism, or the intl. proliferation of weapons of mass destruction by a foreign power; or
    - Clandestine intelligence activities by an intelligence service or network of a foreign power
  + Information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to:
    - The national defense or the security of the U.S.; or
    - The conduct of the foreign affairs of the U.S.
* **Lone-wolf Amendment to FISA (2004)**:
  + Definition of “agent of a foreign power” now includes any non-U.S. person who “engages in terrorism or activities in preparation therefor.” Person doesn’t need to be tied to a foreign power
  + International terrorism involves activities that occur totally outside of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the person they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum
* Contrasting the Wiretap Act with FISA
  + Both Title III and FISA:
    - Prescribe authorization procedures to be followed before electronic surveillance may be conducted (e.g., judicial approval, minimization, and limitations on use of intercepted info)
    - Impose civil and criminal sanctions for unauthorized surveillance
    - Regulation “aural and visual electronic surveillance” but
      * FISA = foreign
      * ECPA = domestic
  + Standard of review in FISA varies greatly from Title III in regards to probable cause
    - FISA requires showing of PC that target is foreign power or agent thereof. Title III requires showing PC for belief that specific individual has committed or is about to commit a predicate crime
    - FISA only requires an official designate the type of intel info being sought and to certify that the information being sought is indeed foreign intelligence information, where as Title III requires PC to believe that information related to crime will be obtained through the interception
    - Title III requires government showing nexus between facilities and communications regarding the criminal offense. FISA only requires PC that facilities have been or will be used by foreign power/agent
  + With respect to notice, Title III requires notice to target once surveillance order expires. FISA only requires notices to persons whose communications were intercepted and are planned to be entered as evidence in proceedings
* Annual FISA report from office of Attorney General
  + In 2014, government made 1,416 applications to FISA, of which 1,379 included requests for electronic surveillance; none of these were denied either in whole or part (nor did they deny any of 170 requests for business records)

### The Wall - *In re sealed case no. 02-001* (2002)

* Facts: first appeal from FISC to the FISA court of review; FISC decision related to surveillance of a known foreign target where the FISA court restricted the type of surveillance that the government could do
* The restrictions were from an assumed barrier between intelligence officials and law enforcement in the executive branch (known as “the wall”)
  + This "wall" emerged from the FISC's implicit interpretation of FISA, most likely out of concerns that FISA may be used to circumvent high standards of domestic surveillance under ECPA
  + FISC had enacted the restrictions to (in their opinion) comply with minimization based on its authority to create procedures designed to prevent acquisition/dissemination of surveillance information unnecessary to foreign intelligence needs; however never referenced any text from FISA nor PATRIOT Act amendments. Government contends that this limitation is neither mandated nor authorized by FISA
  + 50 USC §1805(A): Tthe target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States”
* Holding: FISA (as amended by the PATRIOT Act) support the government’s position and **the restrictions imposed by the FISA court are not required by FISA nor the Constitution** – therefore remand with instructions to grant the applications as submitted (e.g., without restriction)
  + Many courts have relied on the *Truong* court involving electronic surveillance before FISA and based on President’s executive power, and holding the Executive Branch should be excused from securing a warrant only when “object of the from search is a foreign power, its agents or collaborations and “the surveillance is conducted primarily for foreign intelligence reasons” – led to the “primary purpose test”
  + Patriot Act amendments to FISA clearly reflect Congress' intent to facilitate coordination between law enforcement and intelligence. FISA courts failure to acknowledge this or provide a constitutional basis for upholding the wall may be a violation of the constitution itself
    - Patriot Act amendments clearly disproved of primary purpose test, stating that foreign intelligence must only be a **significant purpose**
    - Court still firmly asserts that FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes, though concerns about abuse are unwarranted because even under this process, improper purpose will be clear and thus denied
  + FISA’s general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from onset been distinguishable from “ordinary crime control”. Notwithstanding uncertainty surround presidential authority to direct warrantless foreign intelligence surveillance, **the amended FISA process come close enough to meeting 4A warrant standards and is thus constitutional because the surveillance it authorizes is reasonable**

### *Clapper v. Amnesty International* (US 2013)

* Facts:
  + FISA authorized the United States government to conduct surveillance on non-U.S. citizens that were outside the U.S.
  + Amnesty International (Ps) are lawyers, journalists, and human rights researchers, among other things, who do work that often has them communicating with individuals abroad that there was an “objectively reasonable likelihood” to be subject to surveillance under FISA. Further, given the risk of surveillance, they had to spend significant funds to ensure that their communications were kept confidential The plaintiffs brought suit seeking a declaratory ruling that this portion of FISA was unconstitutional
* Holding and Reasoning (Alito, J.):
  + Threatened injury must be certainly impending to constitute injury in fact for purposes of Article III standing
  + To establish standing, a party must establish that its injury is “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.” More specifically, threatened injury must be certainly impending to constitute actual or imminent
  + In the present case, the plaintiffs do not present any evidence that their communications have been intercepted by FISA. To the contrary, they merely claim that there is an “objectively reasonable likelihood” that their communications will be intercepted in the future. However, the plaintiffs have no knowledge of how the government uses or plans to use this portion of FISA
  + For the plaintiffs’ speculations to come true, government must plan to target P's under FISA powers, get FISC approval, and successfully intercept communications that were initiated by P
  + Thus, **Ps do no more than speculate that the surveillance may occur in the future and that is not sufficient to meet the standing standard**. The argument that they have incurred costs due to fear of future surveillance also fails; **can't “manufacture standing” by spending money in anticipation of a harm that is not certainly impending**
* Dissent (Breyer, J.):
  + The majority’s construction of the word “certainly” is too rigid; in actuality it should be construed as “reasonable probability” or “high probability.” Record shows that the possibility of interception under FISA is more than just speculative, but reasonably likely considering the nature of their communications. Thus, this standard for standing is met

### ACLU v. Clapper (2d Cir. 2015)

* Background:
  + The NSA had a program that collected domestic telephone metadata in bulk and on a daily basis, including: (1) the caller’s and recipient’s numbers; (2) the date, the time, the user or device making or receiving the call, and the duration of the call; (3) limited location information; and (4) calling-card numbers. The metadata did not include the content of the telephone call. The NSA received authority for the program from FISC pursuant to § 501 of FISA, as amended by § 215 of the PATRIOT Act
  + Plaintiffs challenge the legality of the bulk telephone metadata collection program, seeking a preliminary injunction to halt the program
  + Court must decide if collection of telephone metadata exceeds the scope of § 215 of the USA PATRIOT Act as it was intended by Congress
  + Federal district court dismissed complaint and plaintiffs appealed
* Holding and Reasoning:
  + **The NSA’s bulk collection of telephone metadata exceeds the scope of § 215 of the PATRIOT Act**
  + Unlike in *Amnesty Intl*, Ps have standing here since it can be demonstrated that their call records were among those collected, thus the surveillance goes beyond impending but has already taken place. From a standing perspective, NSA's activity is most appropriately challenged as a seizure. However, there is also adequate standing to assert a 1A claim, through the direct effects and indirect "chilling effects" that this surveillance has
  + Government concedes that the data collected by the bulk-collection program is not tied to any authorized investigation and is not relevant to a broader threat to national security. Records demanded are not of suspects or those thought to be associated with suspects in an investigation. Rather, the government contends that the data may allow the NSA at some point in the future to identify information relevant to an investigation. It argues that "relevance" is a broad and generous concept under which this activity is justified
    - Court finds government's expansive concept of "relevance" to be both unprecedented and unwarranted
    - Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans
    - This fails even the permissive "relevance" test
  + This expansive interpretation of § 215 is not what Congress intended. If it had been, it would have been expressed unambiguously in the statute after being subject substantial debate
  + The plaintiffs also argue that the bulk-collection program violates the First and Fourth Amendments. However, because the program is not authorized by § 215, there is no need to reach the constitutional issues
* Notes: Re-authorization of bulk collection
  + USA Freedom Act was signed in 2015; restrains some communications surveillance practices revealed to the media by Snowden
  + FISC later re-authorized the bulk collection program for the transition period leading up to the USA Freedom Act taking effect
  + FISC concluded that *ACLU v. Clapper* was not binding on itself and disagreed with the court's analysis. It interpreted USA Freedom act as congressional intent to permit such activity until statutory authorization was set to expire

## All Writs Act

* Provides that: “The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.”
* As of 1977 Court had repeatedly recognized the power of a federal court to issue such commands under the All Writs Act as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued
  + “This statute has served since its inclusion, in substance, in the original Judiciary Act as a ‘legislatively approved source of procedural instruments designed to achieve “the rational ends of law.”’

### United States v. New York Telephone Company (1977)

* Facts
  + Federal Court in SDNY issues order authorizing FBI to install pen register on phone lines and directing D to furnish information and technical assistance necessary to install them unobtrusively (they would be compensated by FBI in return for assistance)
  + FBI had PC that illegal gambling operation was being run out of a facility. D provided FBI information about lines necessary to install pen register, but declined to lease lines to FBI so it could install them unobtrusively. The only alternative would have alerted suspects as to the surveillance
  + D moved to vacate the order that they provide technical assistance arguing that such direction was not authorized under All Writs Act
  + D's motion was initially denied but overturned by CoA, who concluded that courts should not embark upon such a course without specific legislative authorization.
* Issue - Whether a United States District Court may properly direct a telephone company to provide federal law enforcement officials the facilities and technical assistance necessary for the implementation of its order authorizing the use of pen registers1 to investigate offenses which there was probable cause to believe were being committed by means of the telephone
* Holding and Reasoning:
  + The Court recognized **the power conferred by the All Writs Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice and encompasses even those who have not taken any affirmative action to hinder justice**
    - Conforms with principles under which act had historically been applied, which provide that "a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it"
  + Court found that D was a third-party that was not so far removed from the underlying controversy that it could not be compelled, especially with PC that its facilities were being used to facilitate a criminal enterprise
    - Request was not offensive to it and there is no overly-compelling interest in declining to assist
    - No other conceivable means for FBI to accomplish this task
  + Court concludes the **request was consistent with the All Writs Act** and this assistance from utilities is a necessary implication of congressional action authorizing pen registers. Prohibiting the order would unduly frustrate law enforcement and congress' intent in authorizing such surveillance measures
* Dissent
  + Even if order authorizing pen register is valid, dissent does not accept the Court’s conclusion that the District Court had the power under the All Writs Act requiring D to assist in its installation. This conclusion is unsupported by the history, the language, or previous judicial interpretations of the Act
    - It has always been acknowledged that whatever assistance is authorized must be in aid of the court's duties and jurisdiction
    - Governments interest in its investigation is entirely independent of court's interest in its jurisdiction
    - "Plainly, the District Court’s jurisdiction does not ride on the Government’s shoulders until successful completion of an electronic surveillance"
  + While the request at hand is inoffensive, the order is deeply troubling as a portent of the powers that future courts may find lurking in the arcane language of the All Writs Act.

# Private Sector Access

## Origins of the Right To Privacy and Privacy Torts

* Warren and Brandeis' first to call for express "Right to Privacy" tort claim
  + Argued for explicit recognition of the "right to be left alone"
    - While also referring to the "sacred precincts of domestic life" in their article, the intrusion into the home wasn't the threat to privacy they emphasized
    - Instead, they stressed the problem of unwanted publicity about private life as the basis for a privacy tort
    - This would protect the individual's interest in "inviolate personality"
* *De May v. Roberts* (Michigan – 1881)
  + Facts: A doctor and a friend travelled to assist a woman in childbirth. Woman consented to friend’s presence, but later learned he was not a healthcare professional at all , and brought suit
  + Holding: Court held that P **had a legal right to privacy of her apartment at such time** and to be free of any violation thereof. The fact that she consented to the friend's presence does not preclude her from recovering, as failure to disclose full identity/character was deceit and thus a wrong by D which lead to substantial damages from shame and mortification. Accordingly, D is entitled to relief
  + Notes:
    - Here, privacy is characterized as a intimate knowledge of one's physical body, the compromise of a woman's modesty, intrusion into private home life, and a shattering of ones expectation of privacy

### *Manola v. Stevens* (NY 1890)

* Facts: Female stage performer’s manager published a photo of her in tights, and she brought suit for violation that “offended her modesty”
* Holding: Woman entitled to relief
* This case was used by Warren and Brandeis to show that courts were already open to the idea of **protecting privacy against unwanted publicity**
  + Violation of female figure's modesty and autonomy to control use of her likeness was evidence that court has extraordinary willingness to protect individual privacy

### Edwin Godkin, “*The Rights of the Citizen to his Reputation*”

* Defense of privacy with elitist undertones
* Doubted the law could adequately incorporate a right to protecting “so ethereal a quality” as sense of privacy
* Embraced both privacy of the apartment and of unwanted publicity (combines *Roberts* and Warren/Brandeis conceptions of privacy)
* Views privacy as a “luxury of civilization,” previously unknown in “barbarous societies”
  + Element in society **which most contributes to its moral and intellectual growth**
* Right to control information about his thoughts, feelings, and private doings is the same as natural right to decide how much to eat, what to wear, etc
* Privacy valued more by some individuals than others (e.g., women more than men)

### Warren and Brandeis, “*The Right to Privacy*”

* “That the individual shall have full protection in person and in property is a principle as old as common law, but it has been found necessary from time to time to define anew the exact nature and extent of such protection”
* There is no doubt in the need to protect privacy
  + The intensity and complexity of life have rendered it necessary some retreat from the world and individuals, under the refining influence of culture, have become more sensitive to publicity, making this all the more important
  + Gossip perverts belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of people
  + Gossip is fed by supply/demand – so protections are needed to curb
* “It is our purpose to consider whether existing law affords a principle which can properly be invoked to protect the privacy of an individual, and if so, to what extent and nature”
  + **Common law indicates a general right to privacy for thoughts, emotions and sensations, especially in the form of intellectual or artistic property** (property as basis for privacy)
    - It secures the right of determining the extent to which thoughts, sentiments, and emotions shall be communicated to others
    - This should not be dependent on the method or medium of expression adopted (i.e. limited to art, music, etc.)
    - These protections are merely an instance of the more general right to be left alone
    - Since common law indicates such a general right to privacy for thoughts, emotions, etc., then **they should receive the same protections**
  + Conclude that privacy rights are not arising from contracts or special trusts, nor the general principle of private property,” but “**rights against the world”**
* Limitations to the right of privacy
  1. Does not prohibit any publication of matter which is of public or general interest - only those that are unwarranted
     + “Protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity, and to protect all persons, whatsoever their position or station, from having matters which they may properly prefer to keep private, made public against their will”
  2. Does not prohibit communication of matter when the publication is made under circumstances that render it a “privileged communication according to laws of slander and libel”
  3. Should not grant redress for invasion of privacy by oral publication in absence of special damage
  4. Right to privacy ceases upon publication by the individual or with his consent
  5. Truth of the matter does not afford a defense
     + “It is not for injury to the individual’s character that redress or prevention is sought, but for injury to the right of privacy”
  6. Absence of malice is not a defense
     + Suggested remedies for violation of privacy include: compensation, injunction

### *Pavesich v. New England Life Insurance* (Georgia – 1905)

* Facts: Photo of man used in ad implying that he had purchased that company’s insurance, which he had not
* Holding: The fact that the man is an artist does not establish a waiver of the man’s right to privacy, and using a man’s image without his permission is a serious invasion of one’s right to privacy
  + Court cites numerous bases for right to privacy
    - Natural law - right to live as one will, provided no interference with others
    - Even Romans recognized the importance of providing protection against physical intrusion on privacy
    - Constitutional - e.g. 4th Amendment
    - Precedent - *Manola*
* Other considerations:
  + Right to live a life of seclusion without interference, if one so choses
  + Realization that one's image is being used is to recognize his liberty has been taken away from and he is now under the control of another
    - Difficult question of where this liberty ends of others and the public begins
  + Nothing from which to infer that D waived rights. Mere fact that he is an artist doesn't do this
  + No semblance of an expression that warrants 1A protection

### William Prosser, *Privacy* (California Law Review, 1960)

* Previously, most privacy cases dealt with where there existed a right to privacy – however now able to form some definite conclusions on the topic
* Law of privacy comprises 4 kinds of invasion of 4 different interests of the plaintiff:
  1. Invasion on P’s seclusion or into his private affairs
  2. Public disclosure of embarrassing private facts about P
  3. Publicity that places P in a false light in the public eye
  4. Appropriation for the D’s advantage of the P’s name or likeness

### Restatement (Second) of Torts – Invasion of Privacy, General Principle (§652A)

1. One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of another
2. The right of privacy is invaded by:
   1. Unreasonable intrusion upon the seclusion of another, as stated in 652B
   2. Appropriation of another’s name or likeness, as stated in 652C
   3. Unreasonable publicity given to the other’s private life, as stated in 652 D, or
   4. Publicity that unreasonable places the other in a false light before the public as stated in 652E

### *Spokeo v. Robins* (2016)

* Facts: Privacy case with grounding in statutory (FCRA) protections. Spokeo (D) operated a “people search engine” enabling users to search for personal information about a subject that is aggregated from many sources. Information it had gathered about P was incorrect. P finds out and files complaint on his own behalf and on behalf of class of similarly situated individuals. District court dismissed for lack of standing. Circuit court reverses on grounds that P's own statutory rights were violated
* Issue: Did the district court err in dismissing Robins’ complaint for lack of standing? Question is one of Article III case or controversy, aka “standing” – which is intended to ensure judiciary is not encroaching
* Holding: Concreteness of injury not necessarily met (does not take its own position on this question). SCOUTS vacates and remands to to Circuit Court for determination of concreteness
* Reasoning:
  + Court applies 3 Part test to determine standing:
    1. There must be **injury in fact**, meaning the injury must be **concrete and particularized**
       - Particularized - Injury must be particular to the individual. Cannot be some generalized grievance
       - Concrete - Some actual or imminent injury to the individual. Although some intangible harms such as risk can be concrete, bare procedural allegations are not
    2. Fairly **traceable to defendant’s challenged conduct**
    3. **Likely to be redressed by favorable decision**
  + The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements. Where a case is at the pleading stage, the plaintiff must clearly allege facts demonstrating each element
  + Court determined that **the dissemination of false information does not necessarily cause concrete injury**
    - Court recognized that while Congress may create a statutory right and “elevate” “intangible harms” that were previously “inadequate at law”, Article III standing requires a concrete injury “even in the context of a statutory violation.”
    - Thus, it does not follow that a person with a bare allegation that a statute was violated can establish Article III standing

## Privacy Torts - Breach of Confidentiality

### *Humphers v. First Interstate Bank* (1985)

* Facts: Closed adoption where biological mother intended to conceal identity from child. Adopted child seeks to contact mother and reaches out to physician that originally delivered her in childbirth for assistance locating her. Physician knowingly gives false statement about biological mother's health so as to justify disclosing sealed health records that would enable daughter to identify her birth mom. Birth mother sues under multiple theories of relief, including breach and invasion
* Reasoning
  + Court distinguishes breach and invasion
    - While both assert right to control information, they depend on different premises. Not every secret concerns personal or private information
    - **Only one who holds information in confidence can be charged with breach of confidence where as an act of tortious invasion of privacy could theoretically be committed by anyone**
    - One theory **recognizes tort of breach of confidence in non-personal confidential relationships**, which would exclude liability for failing to keep secrets among friends and family
      * May be difficulty identifying such relationships. Some commentators suggest the **duty arises in all non-personal relationships "customarily understood" to carry such an obligation**
  + Clear legal constraints that impose such obligations and no privilege of the doctor can allow him to disregard it
* Notes:
  + Strengths of case: Sensitive data, statutory backing, behavior of disclosure, irreversible consequences
  + Challenges in breach of confidentiality: Absence of a statue and problem of appropriate remedy

### *Morris v. Consolidation Coal* (1994 WV)

* Facts: P was injured in workplace accident and is examined by a physician attempting to get worker's compensation. Company (D) goes to physician and shows him videos of P working after injury without showing any signs of it. Physician wrote Worker's Comp a letter stating he is unable to verify D's injuries. Company suspends and ultimately discharge P from work pursuant to CBA. P files suit against both physician and company for breach of and interfering with confidential relationship, respectively
* Issue: Did conduct of physician or company violate confidential relationship?
* Holding: P has valid claim against physician for breach of confidentiality. Also a claim against company for inducing breach if elements of test are met
* Reasoning:
  + Court recognizes validity of ex parte contact with claimant physician in order to expeditiously resolve injury claims, however this communication is limited to the information contained in the written medical reports or other routine inquiries which do not exchange confidential information
  + **While disapproving of fraud, court says this is still not sufficient to ignore principles that prohibit unauthorized ex parte communication between employer and physician**
    - There were proper ways to submit evidence of fraud to Worker's Compensation Fund without unauthorized communication
    - Purpose of this prohibition is to prevent disclosure of confidential information in the first place
    - Patient did not waive this right, thus confidentiality was breached
  + Court holds **there is a claim against third party for inducing breach if:**
    1. Third party knew or should have known about privileged relationship
    2. Third party intended to or should have reasonable known that his conduct would induce physician to wrongfully disclose
    3. Third party did not reasonably believe physician could disclose without violation
    4. Physician does in fact disclose such information

### *Bagent v. Blessing Care* (2007 IL)

* Facts: Tort claim based on HIPAA. Employee of D conducts blood work that reveal P's pregnancy. Outside of work, employee inadvertently reveals to P's sister, a friend, about the news and immediately backtracks after realizing what she had done. Hospital is sued for employee's actions under theory of respondeat superior. Employee also sued in individual capacity
* Issue: Who is liable under what circumstances? (scope of employment question)
* Holding: Summary judgement in favor of hospital is affirmed
* Reasoning:
  + **An act is outside of the scope of employment if it has no connection with the conduct the employee is required to perform**
    - However, employer can't avoid vicariously liability for act within employee's scope of employment merely by telling them to act carefully
    - **The fact that hospital expressly prohibited the act supports finding that the prohibited act is outside scope of employment**
    - Employee was in no way attempting to serve her employer in disclosing the information, she merely incorrectly assumed that sister had already known

## Privacy Tort - Psychotherapist-Patient Relationships

* **Tarasoff Rule**
  + Therapists are expected to keep patients' secrets, though required by state law to report child abuse/neglect that they learn about
  + State law might also impose requirement that therapist report to potential victims evidence that a patient has imminent plans to commit murder or other serious harm
    - Comes from *Tarasoff v. University of California*, which established rule of negligence liability which imposed civil duty of care
    - Thus, **mental healthcare providers are expected to warn third parties of threats patients make to inflict serious bodily harm to others**

### *Jaffee v. Redmond* (1996)

* Facts - On-duty police officer (Redmond) responds to an incident and shot (and killed) a man whom she claimed brandished a knife and chased another person. Estate brings a §1983 claim against Redmond. In discovery, it is revealed that Redmond had participated in several counseling sessions with a clinical social worker. Records of these sessions are requested by P to the objection of both Redmond and the therapist. After resisting discovery, judge instructs jury to presume contents of these records would be unfavorable to Redmond
* Issue: Can privilege baed on a confidential relationship be asserted here? **Does confidentiality in this relationship promote sufficient interests that outweigh the need for probative evidence?**
* Holding: Yes, Court held that there is a protected psychotherapist-patient privilege in court
* Reasoning:
  + Court acknowledges fundamental maxim serving as foundation for discovery ("that the public has the right to every man's evidence"), though recognized that exceptions exist and are justified by a public good which outweigh that general principle
  + Psychotherapist-patient privilege is rooted in the imperative need for confidence and trust. Necessary for effective treatment, which depend upon patient willingness to make frank and complete disclosures of facts, emotions, thoughts, etc
  + **The mere possibility of disclosure may impede development of the confidential relationship needed for successful treatment**
  + Mental health is a public good of transcendant importance and evidentiary benefit of denying privilege would be modest
* Scalia Dissent
  + Majority position comes at significant cost of occasional injustice
  + Not clear to him that denying privilege would be unacceptable state of affairs and there is a slippery slope in extending this privilege on this basis

### Moravek v. US (2008 SC)

* Facts: P tells psychiatrist he is thinking about going to courthouse, where he is scheduled for appearance, and taking out secret service agents. Psychiatrist discusses with hospital counsel, who makes inquiry with federal court. US attorney's office subsequently requires records, which leads to arrest warrant being issued. P seeks damages on several theories. State of S.C. limited in what it recognizes, so no tort for disclosure to one or a few people
* Issue: Does P have right to relief on any of the causes of action?
* Holding: No. Summary judgement granted in favor of D
* Reasoning:
  + Court recognizes exception to privilege identified by SCOTUS in *Jaffee* where serious threat of harm to patient or others can be averted by therapist
  + No invasion of privacy under any of the recognized torts in state of SC
  + Applying *Tarasoff*, a special relationship exists where D has the ability to monitor/supervise/control an individual's conduct and this is the basis for duty to warn potential victims when specific threat of harm is directed at them
  + **Must be a specific threat to harm a readily identifiable third party**. Here, this is satisfied as the place, time, nd parties wer all identified

### Gracey v. Eaker (2002 FL)

* Facts: Couple sues psychotherapist who sabotaged their marriage by informing each one what the other had said in individual therapy sessions. Bring claim for emotional damages that have resulted from the fallout of their marriage
* Holding - Court rules that P's have properly stated recognized claim
* Reasoning
  + Impact rule inapplicable in fiduciary duty and statutory cases where duty of confidentiality was breached
    - Impact rule requires emotional damages in negligence action demonstrate that emotional distress flowed from physical injuries sustained in an impact
    - Intended to keep from opening the floodgates of purely emotional damage cases
    - Exceptions to this rule are recognized torts where damages tend to be mostly emotional (e.g. defamation, invasion of privacy, etc)

## Statutory Law and Fair Information Principles

* Regulation is sectoral: some sectors escape regulation, such as e-commerce and social media
* Concerns over stifling information flows, innovation, and growth of self-regulation

### Fair Information Principles or Practices

* Have powerfully influenced the development of modern privacy law. They define rights and responsibilities and aim to correct information asymmetries in the collection and use of personal data
* Can be viewed as a set of practical guidelines for constraining the collection, maintenance, use, and disclosure of personal data
  + Creators intended a body of enforceable standards similar to Fair Labor Standards, as opposed to an articulation of high level aspirational principles
  + Original FIPs and OECD guidelines noticeably omitted Notice and Choice. These two "principles" seem to be at odds with original purpose of FIPs of establishing ongoing obligations associated with data collection of use. These simply operate as a waiver/disclaimer, a mechanism to obtain consent for the use of personal data
* The original 5 (1973):
  + Openness - No secret personal-data recordkeeping; no secret systems
  + Individual Access - Individuals must be able to access info stored and know how it is being used
  + Individual Participation - Person must be able to correct or amend the substance of information maintained about them
  + Use Limitation - Limit types of info collected and prevent info obtained for one purpose being used for another without individual’s consent
  + Use Limitation - Ensure data reliability and limitations for intended use and take reasonable precautions to prevent data misuse
* OECD Guidelines add 3 more (1980):
  + Disclosure limitation - Limits on external disclosures of information about the individual
  + Information Management - Responsibility for establishing reasonable/proper polices and practices which assure lawful and necessary use of data collection, use, and sharing and that information is current/accurate
  + Accountability - Organization accountable for its personal-data record-keeping policies, practices, and systems
* Today’s Fair Information Principles or Practices
  + Notice – transparency value; individuals know what info others have; institutions must assess data
  + Appropriate or Expected Use – blocks off choice and gives areas for use
  + Choice – opt-in (not shared w/o consent) versus opt-out (shared unless otherwise requested)
  + Other Uses and Policy Priorities – doesn’t benefit person, but good for society (i.e. health outbreak)
  + Access and Amendment or Correction – correct and review information maintained
  + Minimization – limit who can see info; only get what you need
  + Security and Breach Notification
  + Enforcement – make sure privacy laws are being followed
* Privacy by Design - Goes beyond the FIPs ("raises the bar"). Presents top-down design-thinking approach to privacy, can be viewed as reference framework for more building more detailed criteria
  + **Proactive not Reactive; Preventative not Remedial** - Activities that seek to avoid or reduce risk before it arises rather than respond to it (e.g. centralized governance, external stakeholder engagement, identifying deficient practices, etc.)
  + **Privacy as the Default** - Minimize collection and usage to that which is necessary, maximum amount of privacy afforded to users by default
  + **Privacy Embedded into Design** - Integrate privacy into development lifecycle, change management, and process design
  + **Full Functionality** - Not a zero sum approach, no unnecessary tradeoffs between privacy and functionality (easier said than done)
  + **End-to-End Security** - Protection throughout entire data lifecycle without gaps in accountability
  + **Visibility and Transparency** - Readily available and well defined practices/standards and assurance that they are operating/adhered to as intended (i.e. independent verification)
  + **Respect for User Privacy** - Building a culture of privacy. Concern for user privacy is always at the forefront and guides decisions

### Federal Record-Keeping Privacy Statutes

* **Freedom of Information Act (FOIA)**
  + All persons have right to inspect and copy records and documents maintained by any federal agency, federal corporation, or federal department
  + Notable Exemptions:
    - (6) Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy
    - (7)(C) Records or info compiled for law enforcement purposes…which could reasonably be expected to constitute an unwarranted invasion of personal privacy
* **Privacy Act of 1974**
  + Justification:
    - Individual privacy is affected directly by collection, use, and dissemination of personal information by Federal agencies
    - Thereat to privacy magnified by increasingly sophisticated technology
    - Opportunity for employment, insurance, and credit, right to due process, and other protections are endangered by misuse of certain information systems
    - Right to privacy is a fundamental right protected by constitution
    - Necessary and proper to regulate such activities in order to protect privacy
  + Does the following:
    - Permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by federal agencies
    - Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent
    - Allow an individual to access and correct his personal data maintained by federal agencies
    - Ensure that information is current and accurate for its intended use, and that adequate safeguards are provide to prevent misuse of such information
* Applicability and Scope
  + Applies to federal agencies, not to state or local agencies, or business or private sector organizations
  + Applies only to information about an individual that is part of a federal "record" or "maintained" in a "system of records"
  + Any alleged violation must show that agency breached duty imposed by act, information must have been identifiable and contained within federal record system, and adverse impact resulted from violation and was willful and intentional

### *United States Department of Justice v. Reporters Committee for Freedom of the Press* (1989)

* Facts: The FBI maintains a database of criminal rap sheets. CBS reporter seeks FBI rap sheets of a private family, which controlled a company that seemed to be a front for criminal activity, through a FOIA request. The rap sheet compiles lots of public records about the individual in one place. The argument was that information of the rap sheet was publicly available through different sources, so there was no privacy interest
* Issue: Is the individual privacy interest at stake the type Congress intended to protect with exemptions from the FOIA?
* Holding: Court grants DOJ summary judgement because FOIA has an exception for violations of personal privacy. FOIA was established to provide transparency into government activities for the public, not to violate the privacy of individuals. This is an unwarranted invasion of privacy
* Reasoning
  + FOIA identifies 9 exemptions to the broad disclosure requirements, including 7(C) which excludes records or information compiled for law enforcement purposes, "but only to the extent that the production of such...could reasonably be expected to constitute an unwarranted invasion of personal privacy."
  + Privacy is about the individual’s control over information relating to himself or herself
    - There is a privacy interest in keeping facts out of the public eye and just because an event is not wholly private, it does not follow that there is not some privacy interest
    - Difference between going out and getting information from different sources (no privacy interest) and getting it from a centralized location (privacy interest)
      * Substantial privacy interest in the information of a rap sheet because it provides an easy means of accessing information that previously would have been forgotten
      * Similar to argument about surveillance in *Jones*
  + The release of information under the FOIA was meant to further public scrutiny of the government. This interest is not served by disclosing information about private individuals, but which reveals little or nothing about an agency’s conduct
    - While there is some public interest into the activity of the family, it falls outside of the scope of the FOIA
  + “A third party’s request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen’s privacy, and that when the request seeks no official information about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is unwarranted.”
* Concurrence: Doesn’t like the broad rule established. Thinks that the disclosure of a rap sheet could be justified in certain instances, e.g. when it involves a candidate for public office
* Notes:
  + Mosaic theory: bits and pieces combine to provide a wealth of information
  + Practical obscurity: just because info is out there doesn’t mean it is readily available
  + This case is pre-Google; now, value is in true and accurate information as
  + Think about the difference between transfers of information between the government and private persons vs. intra-government (catching criminals and those defrauding the government)

## HIPAA

* Medical information is perceived as one of the most sensitive types of information. Disclosure of this information can lead to discomfort, embarrassment and discrimination. Confidentiality of the patient-provider relationship encourages people to seek vital medical attention and to be honest about their health concerns
* State statutes and tort law had historically provided remedies for breach of this information, though federal medical privacy laws are a more recent development

### HIPAA Overview

* Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996
  + Main purpose was designed to facilitate portability of health information between providers, payers, etc
  + Privacy/confidentiality concerns implicated in promoting transmission of health information, thus a section of HIPAA intended to address this
  + Through HIPAA, Congress delegated authority to enact national data privacy and security standards to HHS. HHS Office of Civil Rights (OCR) is responsible for implementing and enforcing privacy rules
    - Act authorized HHS secretary to provide recommendations on national health privacy standards and if Congress failed to pass federal health privacy legislation by 1999, HHS would be authorized to promulgate its own standards
    - Congress failed to pass legislation before deadline, thus HHS promulgated its own standards through administrative rule making process
* Amended through HITECH Act in 2009 to: strengthen individual level of control over information; broaden definition of covered entities; increase duties of business associates; create new breach notification obligations; add restriction on sale and marketing of health information; require development of new guidelines regarding limited and de-identified data sets; and increase violation penalties and add no enforcement provisions
  + Under broadened post-HITECH definitions, a breach occurs if there is unpermitted access, use, or disclosure of PHI unless low probability of PHI compromise
    - Nature and extent of PHI involved – likelihood of re-identification
    - Unauthorized person or to whom PHI was disclosed
    - PHI actually acquired or just viewed
* Preemption - HIPAA only a baseline of privacy protections. States can and almost do have more stringent requirements
  + HIPAA expressly provides that it not supercede any provision of state law related if it imposes more stringent requirements

### HIPAA Scope

* HIPAA privacy rule applies to **covered entities**, which includes:
  + Health plans: An individual or group plan that provides, or pays the cost of, medical care
  + Health care clearinghouse: A public or private entity that processes health information received from other entities into various formats
  + Health care provider: Provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business
  + Note: Definition of "covered entity" does not extend to public health/free clinics or pharmacies. These are the two most notable omissions, though this does not appear to be an intentional carve out
  + Note: This is also contingent on
* Covered entities are prohibited from using or disclosing **individually identifiable protected health information** without consent, except as provided in the rule. This information is defined as:
  + Any information...in any form or medium, that is created or received by a [covered entity], public health authority, employer, life insurer, [or] school or university...and relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual
  + Thus, to fall under protection of HIPAA:
    1. Must relate to past/present/future health condition, provision of health care, or payment for provision
    2. Does or reasonably could identify an individual
* A **business associate** (BA) is any person or entity that, on behalf of a covered entity, creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information
  + In order to be covered by HIPAA, a BA must have entered into business associate agreement
  + The HITECH Act makes business associates directly liable for compliance with certain aspects of HIPAA Privacy and Security Rules and makes these entities subject to HIPAA and HHS enforcement
    - Subcontractors now considered BAs and subject to the same HHS enforcement
    - Ensures that the privacy and security protections of the HIPAA rules extend beyond covered entities to those entities that create or receive protected health information in order for the covered entity to perform is health care functions
* There are no restrictions on the use or disclosure of **de-identified health information**, which neither identifies nor provides a reasonable basis to identify an individual
  + De-Identification Requirements
    - Very low probability of identifying persons with info from generally accepted statistical and scientific principles
    - Removal of 18 data elements
      * Name, fax, phone, email, SSN, MRN, health plan no., acct. no., most geographic subdivisions smaller than state, all dates other than year, and biometric identifiers
      * The removal of dates is something that creates challenges for research and public health reporting

### HIPAA Enforcement

* HHS can impose monetary penalties or impose restrictions/corrective actions and monitor the entity’s adherence to them
* HIPAA provides for civil and criminal penalties
  + Civil Penalties
    - Range anywhere between $100 to $1.5MM per violation. Awareness, severity, and corrective measures all taken into account
      * Unknowing violations or reasonable cause ($100 - $150k)
      * Willful neglect ($10k-$50k if corrected; minimum of $50k if uncorrected)
    - HIPAA does not provide a private right of action to individuals whose information was subject to a violation
      * HHS must bring the enforcement
      * Individuals may file a complaint with HHS about a violation of HIPAA
  + Criminal
    - A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment
    - Penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses
    - Increase to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm
* Corrective Action Plans
  + Involve creation and implementation policies to require reasonable administrative, physical, and technical safeguards
  + Back and forth to gain approval by HHS
  + Produce a final report
* Other enforcement measures that can be taken by HHS
  + Investigating complaints filed with it
  + Conducting compliance reviews to determine if covered entities are in compliance, and
  + Performing education and outreach to foster compliance with the Rules' requirements (e.g. letters of technical assistance)

### *Acara v. Banks* (2006 5th Cir.)

* Facts: P sues physician for disclosing medical information during a deposition without her consent. Filed complaint in federal court with violation of HIPAA as the sole basis of federal SMJ. Federal court determined that HIPAA does not provide private right of action and dismissed the case for lack of SMJ. P appealed
* Rule: **Congress must intend to provide private remedy for violations of a federal law in order for an individual to have a private right of action**
* Holding: Statutory language and purpose are strongly indicative that Congress intended to preclude private right of actions arising out of HIPAA violations (e.g. by delegating enforcement to HHS). P fails to meet burden of showing that congress intended the contrary. Thus, court affirms the dismissal

### HIPAA Privacy Rule

* PHI must be kept confidential and cannot be used or disclosed without a person’s authorization (consent) with the following **exceptions** (aka allowances):
  + Treatment, payment, and healthcare operations (TPO)
  + Judicial and administrative proceedings
  + Reporting abuse
  + Avert serious health or safety threat
  + Health oversight activities and public health reporting
  + National Security/Intelligence and Presidential protective services
  + PHI may be disclosed for a law enforcement purpose to law enforcement officers without authorization if in compliance with a court order or warrant, or subpoena or summons issued by a judicial officer, or a grand jury subpoena, or an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by law. Requirements must also be met:
    - Information sought relevant and material to a legitimate law enforcement inquiry
    - The request is specific and limited in scope and purpose to the extent reasonably practicable in light of the purpose for which the information is sought
    - De-identified information could not reasonably have been used
* A person’s authorization must be written and signed. The form must be in plain language and identify the information to be disclosed
  + Cannot condition treatment on authorization to disclose PHI. Exceptions:
    - Research-related disclosure can be a quid pro quo for treatment
    - Treatment may be conditioned if authorization is necessary to determine whether the individual is eligible for benefits or enrollment under a health plan, and for underwriting or risk rating determinations
    - Payment of a claim or benefits can be conditioned upon authorization if the disclosure is necessary to determine a payment and is not for the use of disclosure of psychotherapy notes
* For certain types of uses and disclosures, informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object
  + Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures if it is in best interest of the patient based on their professional judgment
* **Minimum Necessary Rule**: When using or disclosing protected health information, covered entities must “make reasonable efforts to limit protected health information to the minimum necessary” to accomplish their goal
* Covered entities and business associates must have written policy and procedures to comply with HIPAA
* Authorization is required for the use and disclosure of health data for marketing of items and services
* Authorization is required for “any use or disclosure of psychotherapy notes” even if that use is for treatment, payment, and health care operations.”
* **Rights of Individuals**
  + Individuals have a right to access any PHI that is used in whole or in part to make decisions about the individual
  + People can request that their records be amended or request restrictions on the use or disclosure of health information by all covered entities
    - Individuals also have the right to require covered providers to accommodate their requests about how providers communicate with the individual
  + People have a right to file a complaint to the covered entity or to HHS alleging a HIPAA violation – without being retaliated against for doing so

### *Citizens for Health v. Leavitt* (2005 3rd Cir.)

* Facts: P, along with several other associations and citizens, bring suit against HHS challenging the routine use exception under the HIPAA Privacy Rule. They argue that allowing use and disclosure for purposes of treatment, payment, and operations without prior patient consent violates individual privacy rights
* Holding - Court affirms district courts decision to grant summary judgement in favor of D
  + Court addresses each of the bases that P rests its challenge on
    1. DPC of 5A - No violations can be ascribed to the government - any violations of DPC would have been occurred in hands of private entities
    2. 1A infringement of right to confidential communications - any chilling effect on communication does not derive from action of the government
    3. Exceeding statutory authority to promulgate rules - HIPAA requires HHS to balance health care efficiency and privacy protection, which is exactly what this routine use exception is doing
    4. APA violation because rule making was arbitrary and capricious - only arbitrary and capricious if completely ignoring important aspects of the problem, offering justification that contradicts evidence, or relying on inappropriate factors, none of which DHS did

### Impact of HIPAA Outside of Health Care Provision

* How Research Works under HIPAA
  + Research allowed with patient authorization
    - Authorization must be specific
    - Will delay research but still believe in consent
  + Can have research where the authorization requirement is waived by the Institutional Research Board based on a determination that:
    - Minimal risk to privacy because of an adequate plan
    - Research could not be conducted without waiver
    - Research could not be conducted without the data
* How Marketing Works under HIPAA
  + Marketing definition: to communicate about a product or service in a way that encourages purchase or use of the product or service. Exceptions:
    - Reminders to refill prescriptions
    - To recommend an alternative treatment/therapy, but only if no renumeration received
  + Authorization required if “marketing” (including any renumeration) except:
    - In face to face communications
    - With items of nominal values. E.g. pens
* How Law Enforcement Works under HIPAA
  + Pursuant to process (court order, grand jury subpoena, special administrative subpoena)
  + Limited information to locate a suspect, fugitive, material witness, or missing person
    - Identifying info. such as name, height, weight, etc
  + Victims of a crime
  + Can get information on decedents 50 years after death
  + Can get information based on crimes on premises

### Security and Breach Notification Rules

* Security Rule
  + Protects only electronic health info; digital records, but not paper records (as of 2005)
    - Protect against reasonably anticipated threats or hazards to the security and integrity of [e-PHI]
  + Requires covered entities and BAs employment certain safeguards
    - Administrative – Risk analysis and management, access auth, security training, and security incident plans
    - Physical – Facility security plan, access limits to records, safe disposal and data backup processes
    - Technical – Login authentication, encryption, and audit controls
  + Link: [Mapping HIPAA Security Rule to NIST CSF, NIST 800-53, and ISO 27001](https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf)
* Breach Notification Rule
  + Requires individual to be notified if their PHI is involved in a data security breach
    - Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted… which compromises the security or privacy of the PHI
  + Individuals must be notified without reasonable delay
  + Presumed to be a breach unless the covered entity can show a low probability that the protected health information has been compromised based on risk assessment. Four non-exclusive factors:
    - The nature and extent of the protected health information involved, including the types of identifies and the likelihood of re-identification
    - The unauthorized person who used the protected health information or to whom the disclosure was made
    - Whether the protected health information was actually acquired or viewed
    - The extent to which the risk to the protected health information has been mitigated

## Genetic Information Privacy

* Genetic information is a subclass of medical information which can be retrieved from DNA to reveal following classes of sensitive information:
  + Personal information about the individual such as genes, traits, predispositions, etc
  + Medical information about kinship that can be attributed to one's genes
  + Information about the heritage of the individual (i.e. genetic ancestry)
* Development in technology and science related to genetic information has lead to numerous tangible benefits in the health care space. Care is more effective and targeted, costs will be lowered, profitable research uses, and increased market efficiency. However, increased proliferation of genetic information has enlarged existing privacy concerns and raised new ones
* Why we care about genetic information
  + Can reveal medical history, future health via gene linkage, and info about whole family
  + Many want to keep themselves from seeing this information in addition to others (e.g. adopted individuals)
  + Discrimination may result based on genetic information (e.g. denial of insurance because of high predisposition to costly disease)
    - Note: Basing employment decisions on genetic testing for future disabilities is a violation of the ADA
  + Free market may fail to adequately protect it because it fails to account for social externalities in the form of genetic determinism and attached stigma
* Conceptions of and legal/philosophical bases for genetic privacy
  + Personal property argument - Advanced in *Moore v. UCLA*, which asserted that if courts have held individuals have property interest in their own persona, then surely this would translate to similar right over over genetic information. Court ultimately rejected this
  + Future diary metaphor - may be predictive of future diseases and even lifespan, offering a probabilistic peek into future health. The value and effectiveness of genetic information as a predictor of future health has been widely disputed
* Genetic Information Non-Discrimination Act
  + Prevents insurance companies and employers from using genetic tests to deny individuals health coverage or employment
    - Built on the existing protections of HIPAA which had partial protection from discrimination on the basis of genetic information
  + Prohibits genetic information in health insurance by forbidding insurers from adjusting “premium or contribution amounts” on the basis of genetic information
    - Effectively makes genetic information "health information" and thus subject to the restrictions on use and disclosure in HIPAA
  + Also prohibits employment discrimination on the basis of genetic information
    - It is an unfair employment practice for an employer “to fail, or refuse to hire, or to discharge, any employee, or otherwise to discriminate against any employee” because of genetic information
    - Further prohibits an employer from requesting, requiring, or purchasing genetic information about any employee, subject to a few exceptions
* Issues related to usage in research and consent
  + Ability to replicate DNA gives rise to possibility that it be used for purposes other than those for which they were originally intended. Additionally, extraction of genetic information derived from genetic material/DNA into a large centralized database creates even greater privacy risks
  + Genuine informed consent can only be given if the research subjects understand and agree to the general nature of the research, are asked for additional consent for each different future usage, and the ability withdraw from research or object to specific uses
  + Private sector is more problematic because of profit motive. Argument that industry should adopt and abide by FIPs as a result
  + Presidential commission report makes recommendations regarding genetic privacy and consent that approximate something like the FIPs

## FERPA and Education Privacy

* Privacy concerns in the context of education
  + Protecting performance or disciplinary information - this information is commonly used as the basis of many inferences about a person and evaluating their intellectual capabilities. Disclosure without additional context can lead to false perceptions about that person
  + Fostering free exchange of ideas / learning process - may have chilling effect on what goes on in the classroom
* Family Educational Rights and Privacy Act (FERPA)
  + Gives parents certain rights with respect to children's education records, which transfers to student once they reach adulthood
    - Parents/students have right to inspect and review education records **maintained by school**
    - Parents/students have right to request correction of records they believe to be inaccurate or misleading. If declined, they have right to formal hearing and to place statement with the record
    - Schools must have written permission from parent/student in order to release any information from a student's education records. Exceptions: School officials with legitimate educational interests, other schools to which student is transferring, financial aid related parties, research or accreditation organizations, or subpoena

### *Owasso v. Falvo* (2002)

* Facts: Several teachers in the district use peer grading to grade student assignments. D had multiple children enrolled in district, including in classes utilizing such grading methods. D requests method be banned because it embarrassed her children, but district declined. D sues district, claiming it violate FERPA
* Rule: **Under the FERPA, student-graded assignments are not educational records**
* Holding:
  + FERPA requires that schools receiving federal funds comply with certain privacy requirements
    - Educational records cannot be disclosed without the written consent of the student’s parents. Educational records are defined as records, files, and documents related to a student that are maintained by a school or a person acting on behalf of a school
    - FERPA also requires the school to maintain a record of access for each student’s educational records
  + Student-graded assignments are not "maintained" by the school based on the terms ordinary understanding. This is also consistent with the statute's context, as the alternative interpretation would entitle parents to hearing to contest every graded assignment, an intrusion on traditional state function (federalism concern)

### *Gonzaga v. Doe* (2002)

* Facts: John Doe, student in teaching program Gonzaga alleged to have sexually assaulted another student. Program administrator overhead another student talking about the assault. Program director and another school official conduct ad-hoc investigation. However, John Doe was not informed of the investigation against him. Victim is interviewed in investigation, but gives equivocal testimony. After the school concluded its investigation, the Dean of the School of Education concluded John Doe was not fit to be licensed as a teacher due to problems with his moral character application from the incident. The Dean only told John of this a month later, and told him he had no right to appeal the situation. John Doe brought suit against Gonzaga for defamation, but also for the release of personal information to an unauthorized person under FERPA
* Legal Issue: Was John Doe deprived of right not to have education records disclosed to unauthorized persons, and if so, is this right enforceable in suits for damages?
* Rule: **FERPA nondisclosure provisions fail to confer enforceable rights and thus there is no private right of action**
* Holding: No individual private right of action for violation of rights conferred by FERPA. Congress established very unambiguous enforcement scheme - loss of federal funding for failures to comply, in addition to onsite inspection and complaint based investigations

### *Vernonia*, *TLO*, *Earls*, *Safford*

* All address 4A freedom from unreasonable searches and seizures in school setting
* Probable cause also replaced with reasonableness
  + Search actually conducted was reasonably related in scope to the circumstances which justified it in the first place
    - Level of suspicion must match degree of intrusion. Reasonable expectation of privacy factors into the level of intrusion
    - Must not be excessively intrusive in light of the age/sex of the student and the nature of the infraction
  + Do not want to burden schools with full requirements of 4A (e.g. as they apply to law enforcement)
    - A requirement to obtain a warrant before searching a student suspected of a crime or an infraction of school rules would unduly interfere with the school’s need for swift and informal disciplinary procedures
* Threshold of reasonableness of policy
  + Considers degree of reasonable expectation of privacy
    - Students in extracurricular activities consensually subject themselves to greater levels of control and have reduced expectations
  + Considers level of student interest in maintaining privacy
  + Considers school's interest in maintaining order
    - Not necessary that the school use the least intrusive method to achieve its goal. The severity of the need must be viewed in balance with the expectation of privacy and obtrusiveness of the search

## Infosec and Breach Notification

* Cybersecurity
  + Consumer harm from security breaches includes identity theft, but also cybersecurity issues
  + Cybersecurity implicates stealing trade secrets, military info, and infrastructure tampering
* Information Security and Privacy are distinct, but probably compatible. Need security to make privacy viable
  + Privacy – individual’s right to know, choose, see, change
  + Security involves protecting three[3] primary aspects of data
    - Confidentiality - Limit access to authorized parties, prevent unauthorized disclosures
    - Availability – Maintain ability of authorized parties to access important information when needed
    - Integrity – Ensure no changes are made to important information
* Incidents or "breaches"
  + Not limited to large-scale compromise of systems, but small ordinary occurrences where sensitive information is exposed. Examples:
    - Mailing errors, inadvertent printing/faxing/scanning, etc
* What role should the law play?
  + Wide range of intentional and unintentional problems. Landscape is constantly and rapidly evolving
  + Possible models: Prescriptive, guided risk assessments, consequences for failures
* Various approaches
  + HIPAA
    - Scalability - takes into account size/complexity/likelihood/consequences of harm
    - Risk analysis - Measure impact, remediate risk, document/justify correction measures, maintain protection
  + GLBA
    - Streamlined Risk Assessments directed at specific activities required of information security program
  + Breach Notification - Incentive Based Approach
    - Allows actors to employ security measures as they see fit, bearing in mind the consequences of breach
    - Pros - Flexibility and scalability, probably more cost efficient
    - Cons - Some good organizations make mistakes, may underincentivize proper level of care
    - 50 states with 50 different notification laws - varying triggers, time frames, reporting content, etc
    - HIPAA also has breach notification rule
      * An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity demonstrates that there is a “low probability” that the PHI has been compromised
      * Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media

## FTC Enforcement

### FTC Overview

* Federal Trade Commission - Administrative agency that is a subset of the executive branch; broad delegation of authority
  + Has both investigative authority and enforcement authority
* Investigative Authority
  + FTC may prosecute any inquiry necessary to its duties and may gather and compile information concerning, and to investigate the organization, business, conduct, practices, and management of any person/partnership/corporation engaged in business affecting commerce
    - Exceptions: Banks, savings/loan institutions, Federal credit unions, and common carriers
* Enforcement authority
  + Following an investigation, FTC **may initiate enforcement action if it has "reason to believe" that the law is being or has been violated**
  + Primary purpose of enforcement authority is to enforce consumer protection laws. Said to possess "unfairness authority" to prohibit and prosecute unfair acts or practices harmful to consumers
    - Section 5(a) of the FTC Act - "**unfair or deceptive acts or practice in or affecting commerce are declared unlawful**"
      * Rather than enumerate individual unfair methods of competition, Congress intentionally left the development of the term unfair to the FTC through case-by-case litigation
      * However, FTC's interpreted meaning of unfair practices, based on case history, are those that:
        1. **Cause or are likely to cause substantial injury to consumers AND**
        2. **Cannot be reasonably avoided by consumers AND**
        3. **Is not outweighed by countervailing benefits to consumers or competition**
      * Also a public policy component that factors into this determination, though the extent to which is not clear/consistent
        + Looks at the basis of an act's unfairness in common law, statutes, or the constitution in addition to all other evidence
  + **Administrative Enforcement**
    - FTC can challenge unfair/deceptive acts/practices through maintenance of an administrative **ajudication**
      * Where there is reason to believe there is a law violation, may issue a complaint setting forth its charges
        + Respondent can elect to settle charges, it can sigh consent agreement (no admission of liability), consent to entry of a final order, and waive all right to judicial review
      * Once FTC order becomes final, a respondent is liable for civil penalty. District court may also issue mandatory injunctions and other forms of equitable relief
        + FTC may also seek consumer redress from respondent for injury that was at issue in the proceeding
      * Can impose civil penalties on non-respondents who thereafter violate standards articulated by FTC. It must show that violator had "actual knowledge that the practice was unfair/deceptive and unlawful under §5(a). Limits wrongdoers to only a "single bite of the apple" before they are subject to monetary penalties
    - Can also use **rulemaking authority** - using trade regulation rules to remedy unfair/deceptive practices
      * §57(a) authorizes prescription of such rules. Mus provide opportunity for informal hearings and reason to believe practices targeted by rules are prevalent
  + **Judicial Enforcement**
    - FTC must still seek aid of court to obtain civil penalty or consumer redress for violations of its rules or orders to cease and desist
    - §13(b) authorizes FTC to seek preliminary and permanent injunctions to remedy "any provision of law enforced by the [FTC]." Whenever there is "reason to believe" that any party "is violating, or is about to violate" a provision of law enforced by the FTC, it may ask the district court to enjoin the allegedly unlawful conduct, pending completion of an FTC administrative proceeding to determine whether the conduct is unlawful. In proper cases, it may seek, and the court may grant, a permanent injunction
    - Agency adjudication offers certain advantages over direct judicial enforcement. In a adjudicatory proceeding, the FTC has the first opportunity to make factual findings and articulate the relevant legal standard. On review, the court is obliged to affirm the Commission's findings of fact if supported by substantial evidence. A reviewing court must also accord substantial deference to Commission interpretation of the FTC Act and other applicable federal laws. In a 13(b) suit, by contrast, the Commission receives no greater deference than would any government plaintiff
      * Thus, where a case involves novel legal issues or fact patterns, the Commission has tended to prefer administrative adjudication

### In the Matter of Facebook

* Facts: FTC brings enforcement action against Facebook for deceiving its customers with its privacy related promises. In the complaint, the FTC alleges that:
  + Changes were made to the website that made previously private information public without notifying users or getting approval
  + Third party apps could gain user info via “Friend” authorization or exceeding user granted permissions
  + Allowed access to photos and videos uploaded by deactivated accounts despite claiming they would be inaccessible
  + Users could not control own data privacy and disclosure as promised in the privacy policy
  + Claimed that it doesn't share personal information with advertisers or third parties even though it was doing so
* Outcome:
  + Facebook enters settlement agreement which barred them from making any further deceptive privacy claims, requires them to get approval before changing the way it shares data, and required it obtain periodic independent privacy assessments for the next 20 years It also require them to establish and maintain a comprehensive privacy program to address such risks in the future
* Notes:
  + Administrative complaints are issued by FTC whenever it has reason to believe has been violated or is about to be violated and that a proceeding is in the public's interest

### In the Matter of Google

* Facts: FTC settles with Google after charging that the company had been using deceptive tactics and violated own privacy promises to consumers in violation of the FTC Act. FTC alleged that Google's "Buzz" service violated its own privacy policies by using information originally provided to Gmail for another purpose without first seeking consent. Additionally, those who explicitly opted out of the program were still nonetheless enrolled in specific features of Buzz
* Outcome: Settlement barred Google from making any further deceptive claims about privacy or confidentiality of user data and from misrepresenting compliance with various privacy compliance programs. It also required it obtain periodic independent privacy assessments for the next 20 years and to establish and maintain a comprehensive privacy program to address such risks in the future
* Notes:
  + Nearly identical to the settlement reached with Facebook

### In the Matter of Snapchat, Inc

* Facts: FTC alleged the following in the claim it brought against Snapchat:
  + (1) Claimed snaps were gone forever after timer expired; false and misleading
    - Third party apps and computer downloads allowed bypass to save pics and videos
  + (2) Screenshot notifications; false because API work-around allowed bypass of notification
  + (3) No geolocation by Snapchat; false because Android transmitted location info for analytics
* Outcome: Snapchat enters same boilerplate settlement agreement as Facebook and Google did
* Notes:
  + This set of circumstances isn't as clear of a violation as the other ones, as all Snapchat did with screenshots was create a program with features that could be circumvented by individuals using 3rd party software (this isn't exactly a bug, but a design flaw)
    - Issue may be that Snapchat knew about the design flaw and did not take action to fix it
    - Big question here of how responsibility should be allocated. Strict liability?

### *FTC v. Wyndham Worldwide Corp.* (2014 NJ)

* FactsL Property management system hacked on three separate occasions by brute force. Customer personal info stolen because no reasonable safeguards, leading to $10.6MM in losses. FTC alleges unfair practices due to inadequate data security (unnecessary and unreasonable exposure of customer information) and that the privacy policy was deceptive
* Issue: Does FTC have authority to regulate cybersecurity under the "unfair practices" prong and if so, did Wyndham have fair notice of its obligations and that its practices could fall short or FTC's standard?
* Outcome: FTC has sufficient authority over data security and Wyndham had fair notice of requirements
* Rules:
  + **To satisfy finding of unfairness, injury must: be substantial; not be outweighed by countervailing benefits to consumers or competition; and could not have been reasonably avoided**
  + **FTC’s unfairness authority over data security can coexist with existing data-security regulatory scheme**
  + **Public complaints and consent agreements along with published guidelines from FTC provide can provide fair notice**
* Reasoning:
  + Congress does not need to give FTC specific power like in other statutes; can coexist within current framework
    - Authorizing FTC to promulgate sectoral standards does not mean it didn't already have enforcement authority over cyber security under the FTC Act. Nor does its lack of authority to enact universal FIP requirements
  + Court holds that alleged misconduct falls within boundaries of FTC's meaning of unfair
    - Court rejects argument that injury was avoidable because consumers good book with another hotel brand. Consumers had been mislead by privacy policies giving them no reason to consider alternatives with better privacy practices
  + There were clear failures to establish password complexity requirements, to track systems connected to the network and enforce boundary protection to appropriately limit uses
    - Also rejects argument that D can't be liable because it itself was victimized by criminals responsible for the breach. D need not be the most proximate cause of injury if the harm is foreseeable
  + Fair Notice - Wyndham argues it is entitled to ascertainable certainty of FTC's interpretation of required cybersecurity practices
    - FTC has not yet declared that cybersecurity practices can be unfair, this is first time FTC is asking courts to interpret §45(a) in this way; there is no relevant FTC rule, adjudication, or document that merits deference
      * Thus, the case involves ordinary judicial interpretation of a civil statute and **the ascertainable certainty standard does not apply. Relevant question becomes whether Wyndham had fair notice that its conduct could fall within the meaning of unfair under the statute**
    - Court rejects contention that Wyndham did not have fair notice of the specific cyber requirements necessary to avoid liability. FTC had published several guidelines and checklists providing sound cyber practices. It had also filed complaints and entered consent agreements with companies with unfairness violations arising out of inadequate cybersecurity practices. All proposed agreements were published in the federal register
* Note: Result of this case may have been to strengthen FTC’s role in protecting consumer data security

### *LabMD v. FTC* (2018 11th Cir.)

* Facts: FTC had filed complaint that LabMD had committed an unfair act by engaging in a number of practices that, together, failed to provide reasonable and appropriate security for consumer data. This arose out of an incident by which a file containing a large amount of sensitive consumer data was inadvertently published on the p2p file sharing service LimeWire. LabMD moved for summary judgement and ALJ dismissed the complaint, concluding it failed to prove LabMD's alleged failure to employ reasonable security controls lead to substantial injury. FTC appealed and it was reversed after full Commission review, holding unauthorized disclosure caused privacy harm and that mere exposure was likely to cause injury as well. FTC subsequently ordered LabMD implement a security program which would comport with its standard of reasonableness. LabMD appealed, arguing the order does not direct it to cease committing an unfair act within the meaning of 5(a), thus the cease and desist order is unenforceable
* Holding: CoA holds that the the cease and desist order is unenforceable
* Reasoning
  + Court, for the sake of argument, assumes conduct was indeed unfair
    - In theory, failure to provide adequate security measures is grounded in tort law of negligence, so it has basis in public policy
  + Court concludes then considers whether cease and desist order is enforceable - failure to comply with this would make LabMD liable for a civil penalty
    - **Cease and desist order prohibitions must be stated with clarity and precision, else it risks due process violations that would make the order unenforceable**
    - **Order in this case does not contain any prohibitions or does not instruct LabMD to stop committing specific acts**. Instead, it commands them to overhaul security program. This command is unenforceable
      * Devoid of any meaningful standard informing the court which constitutes a reasonably designed security program (i.e. lacks specificity)
      * Narrower order, such as commanding LabMD to eliminate the possibility of employees installing unauthorized software (e.g. LimeWire), would hae been easily enforceable
      * However, complaint uses LimeWire incident as entry point to allege broad deficiencies in security practices as a whole. Used this as the basis of order which would broadly regulate all aspects of LabMDs data-security program

## Financial Privacy

* What is at stake with financial privacy?
  + Being able to ascertain one's wealth shapes perception of that individual
  + What you spend money on:
    - Useful commercial profile
    - Reveals possible illegal, immoral, embarrassing, or misleading activities
  + Concern about theft of identity of funds
  + Finances are your livelihood
* Two major statutes that govern the use of personal information by financial institutions - FCRA and GLB

### *United States v. Miller* (1976)

* Facts: D convicted of operating unregistered whiskey distillery without giving bond (as required by statute) and with intent to defraud Government of whiskey tax and tax revenues. Prior to trial, D moved to suppress copies of checks and bank records that he alleges were obtained from banks via defective subpoenas. Originally denied by trial court, but reversed by CoA who ruled that it violated Fourth Amendment rights
* Rule: **4A does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and that confidence in third party will not be betrayed**
* Outcome: Supreme Court reverses CoA and holds there was no 4A violation
* Reasoning:
  + Court finds no intrusion into any area in which D had protected 4A interest. There was no intrusion into a zone of privacy - the security a man relies upon when he places himself or his property within a constitutionally protected zone
  + Documents subpoenaed were not D's "private papers" as it relates to 4A. D had neither ownership nor possession of these records
  + D invokes *Katz* as a defense (expectation of privacy), but court points out that *Katz* made it clear that what individual knowingly exposes to the public is not subject to 4A protections (this is later the basis of 3rd party doctrine in *Smith*)
    - Considering nature of documents, Court says there is no legitimate expectation of privacy in their contents. They were not confidential communications and exposed to many different employees in ordinary course of business

### Right to Financial Privacy Act (RFPA)

* Right to Financial Privacy Act (RFPA) was enacted in 1978 to "protect customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity
  + Enacted in response to *Miller* in which SCOTUS held there was no constitutional right to privacy of financial records
* The RFPA provides that, unless a statutory exception applies: No Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless:
  + The financial records are reasonably described
  + AND such financial records are disclosed in response to an administrative subpoena or summons which meets the statutory requirements
* Definitions
  + Customer - any person or authorized representative of that person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary, in relation to an account maintained in the person's name
  + Person - an individual or a partnership of five or fewer individuals

### Fair Credit Reporting Act (FCRA)

* Background:
  + Passed in 1970 to regulate consumer reporting agencies. Inspired by allegations of abuse and lack of responsiveness of credit agencies to consumer complaints
  + The FCRA requires credit reporting companies to provide an individual access to her records, establishes procedures for correcting information, and sets limitations on disclosure
* Scope: Applies to any consumer agency furnishing a consumer report
  + Law shaped by the few entities that had large amounts of data at the time - federal government and credit bureaus. It now extends to a much broader set of institutions
* Definitions:
  + **Consumer report** – any type of communication by a CRA bearing on consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living…used or expected to be used to establish a consumer’s eligibility for credit, insurance, employment or other permissible purposes
  + **Consumer reporting agency** – any person, which for monetary fees, dues, or on a cooperative nonprofit basis regularly engages in assembling or evaluating consumer credit info or other info on consumers for purpose of furnishing consumer reports to third parties with expectation that it would be for a consumer purpose
* **Permissible Uses of Consumer Reports**
  + Consumer reporting agencies **(CRAs) can furnish consumer reports only under certain circumstances for certain uses**:
    - In response to a court order or grand jury subpoena
    - To the person to whom the report pertains
    - To a person which the agency has reason to believe intends to use the information in connection with:
      * The extension of credit to the consumer
      * Employment purposes
      * Insurance underwriting
      * Licensing or the conferral of government benefits
      * The assessment of credit risks associate with an existing credit obligation
      * Legitimate business need when engaging in a business transaction involving the consumer
    - To establish a person’s capacity to pay child support
* Liability for individual persons and non-CRAs
  + The FCRA does not only place restrictions on consumer reporting agencies. It **also creates a private right of action for any consumer regarding any person who under false pretenses gains a consumer report, or who willfully or knowingly fails to comply with certain of its requirements (e.g. using for impermissible purpose)**
* Requires maximum possible accuracy, adverse actions notices, and deletion over time (seven years)
  + Must employ reasonable procedures to ensure maximum possible accuracy concerning individual to whom report relates
  + Deletion not applicable for credit transaction > $150k, life insurance > $150k, salary > $75k / yr
  + Accuracy requires nearly perfect record; leads to duties to investigate
  + Bankruptcies are subject to 10 years before deletion rather than 7 years
  + Imposes duty on creditors to reasonably investigate the validity of disputed charges after being notified by CRAs
* CRA must notify the entity to whom it is furnishing a consumer report of their obligations/responsibility under the FCRA
* CRA cannot furnish consumer reports to entities for which it has reason to believe has no permissible purpose for the information under the FCRA
* Rights of individuals under the FCRA:
  + Must be notified if information in report is basis for adverse action. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information
  + Right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (free in many cases, but requires you verify your identity). This also includes the right to know your credit score, a numerical summary of the information contained in the files
  + Right to dispute or request correction to inaccurate/incomplete information. CRAs must correct, remove, or verify within 30 days of the request
  + When an employer or potential employer seeks a consumer report for employment purposes, they must first disclose to you in writing that a consumer report may be obtained, and you must authorize in writing that the report can be obtained (exception in the trucking industry, for whatever reason)
  + Right to place a “security freeze” on your credit report, which will prohibit a nationwide consumer reporting agency from releasing information in your credit report without your express authorization (can create complications if frequently engaged in transactions involving credit checks )
  + The entity seeking the report from a consumer agency must certify that they obtained the consent of the individual and that they will not use the information in violation of any equal employment opportunity law or regulation
    - However, consumer reporting agency can furnish a consumer report, without the consumer’s authorization, if:
      * The transaction consists of a firm offer of credit or insurance
      * The consumer reporting agency has the opt-out provisions in subsection (e) and consumer has elected not to have their name or address excluded from lists of names provided by the agency pursuant to this paragraph (Consumers may opt out of unauthorized disclosures. May opt out for two years by phone or may sign an opt-out form, which lasts till the consumer says otherwise)
* Government agencies under the FCRA - Consumer reporting agency may furnish identifying information respecting any customer, limited to his name, addresses, places of employment, or former places of employment to a governmental agency
  + The FBI can obtain the names and addresses of all financial institutions at which a consumer maintains or has maintained an account by presenting a written request to the consumer reporting agency
    - Also, pursuant to a written request by the FBI, a consumer reporting agency must disclose identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment
    - The FBI, however, must certify that the information is sought in an investigation to protect against international terrorism or clandestine intelligence activities and that the investigation is no conducted solely upon the basis of activities protected by 1A

### *United States v. Spokeo* (2012)

* Facts: FTC filed complaint against Spokeo for sale of information to companies for background checks. Spokeo is an entity that assembles consumer info from online and offline sources to create comprehensive profiles on users. It promoted its product/services to HR, background check and recruiting companies. The basis for the complaint filed by the FTC were:
  + After it modified T.o.S. to state that it wasn't a CRA, there was a failure to revoke access or otherwise ensure that existing users did not use the company's website or information for FCRA covered purposes. Spokeo was thus furnishing consumer reports and functioning as a CRA despite making explicit representations to consumers that it wasn't a CRA
  + It failed to maintain reasonable procedures designed to avoid violations and limit the furnishing of consumer reports to the permissible purposes specified in the FCRA
  + It failed to employ reasonable procedures to assure maximum possible accuracy of the information in reports that it prepared
  + It failed to provide notice to users of consumer reports as to their obligations for using the information under the FCRA (e.g. duty to notify subject of adverse action based on information contained in report)
  + It furnished consumer reports to entities that it had reason to believe had no permissible purpose for the report under the FCRA
  + It displayed comments on public profiles that were represented as reflecting the views of ordinary, independent users when they were in fact created by Spokeo
* Outcome: $800,000 civil penalty for violations of FCRA in settlement agreement
* Takeaways:
  + Measures taken by Spokeo to avoid coverage of FCRA were not enough. If you don't intend to be a CRA, you need to completely stop engaging in practices for any FCRA related purposes
  + Once an entities conduct renders them a CRA under the statute, they become responsible for the full suite of compliance obligations and are liable for any failures to do so

### *Hansen v. Morgan* (1978 9th Cir.)

* Facts: P defeats incumbent in congressional race. During lame duck session, House Admin Committee, of which incumbent was a member, launched investigation into alleged campaign finance violations by P. D, jewelry store owner, gets request to relay credit report on P. Under impression that this was for the purpose of assisting with the investigation, D gets credit report from bureau and delivers it to incumbents office. Upon learning, P files suit for violating FCRA and his right to privacy
* Rule: **Obtaining consumer report in violation of the FCRA without disclosing the impermissible purpose for which the report is desired constitutions as obtaining consumer information under false pretenses**
* Holding: The credit report was obtained in a way that violated FCRA and P has valid cause of action against D
  + Court determines the document falls under FCRA definition of "consumer report": it was written form of communication by a consumer reporting agency bearing on P's credit worthiness/standing and expected to be used for purpose of determining P's eligibility for credit transactions
  + Court says standard for determining whether report was obtained under false pretenses is whether the desired purpose for obtaining the report is permissible under the FCRA
    - CRAs can only legally issue reports for permissible purposes enumerated in the statute. Thus, since D's purpose for obtaining the report was impermissible, he only could have obtained it under false pretenses
    - Facts demonstrate that the report in this case was obtained under false pretenses and thereby forms basis of civil liability

### *Yohay v. City of Alexandria Employees Credit Union* (1987 4th Cir.)

* Facts: Ex-spouse wants access to credit reports on P to ensure he was no longer using joint credit cards. Credit union, which had contract with credit bureau, had no rules that governed obtaining reports or restricting access. P became aware when he saw credit union that he had no affiliation with had performed credit check on him. Files suit against credit union for violating FCRA
* Holding - Credit union is liable to P for willful failure to comply with FCRA
  + If willfully failed to comply with FCRA, D is liable to P for both actual and punitive (as court may allow) damages as well as attorney's fees
  + Record shows sufficient evidence to support conclusion that credit union acted wilfully. Friendly relationship between credit union manager and ex-spouse suggests he was cognizant of the impermissible purpose
  + Failing to employ any safeguards and effectively allowing anyone to request/access files furnished by credit bureau factored into courts awarding of punitive damages - this is meant to deter

### *Thompson v. San Antonio Retail Merchants Asso.* (1982 5th Cir.)

* Facts: Similarly named individuals had files mixed up in credit reporting system. Impossible to determine which information was attributable to each of the two different persons. As a result of the mixup, adverse information from one individual caused another to get denied credit over course of several months. Even after it was discovered, it took several months and pending lawsuit to get corrected
* Holding: D is liable for non-economic harm caused by its violation of the FCRA
  + Clearly violated compliance requirement to ensure maximum possible accuracy in neglecting to employ procedures to discover or promptly correct egregious errors
  + **Actual damages awarded by lower court based on humiliation and mental distress do constitute as recoverable elements of damage under the FCRA**
    - Record shows that trial judge was entitled to conclude should damages were substantial

### *Johnson v.MBNA* (2004 4th Cir.)

* Facts: P's ex-spouse had account for which he owed several thousand dollars on but was removed from the account after filing for bankruptcy. Dispute as to whether P was co-obligor on account, making her legally obligated to pay off balance, or merely an authorized user. D, credit card company, concluded she was obligated and affirmed dispute verification after P contested the debt with big 3 agencies. P brought suit for failing to conduct proper investigation in violation of FCRA
* Rule: **FCRA requires creditors, after receiving notice of consumer dispute from rating agency, to conduct reasonable investigation into their records to determine if disputed information can be verified**
* Holding - Court affirms trial court finding that D violated FCRA in failing in its duty to conduct reasonable investigation
  + Plain meaning and legislative history supports interpretation that investigation must be more than superficial/perfunctory
  + Jury could reasonably conclude that D failed to act reasonably in its attempt to verify the information - nothing beyond the contents of the original records were consulted during the pseudo-investigation

### Gramm-Leach-Bliley Act (GLB)

* Legislation passed in 1999 authorizing widespread sharing of consumer personal info by financial institutions
  + Financial institutions - companies that offer financial products or services to individuals such as loans, financial/investment advice, or insurance
  + Only protects financial information that is **not public**
* 3 principal parts to the privacy requirements: financial privacy rule, safeguards rule, and pretexting provisions
  + **Financial privacy** governs collection and disclosure of customer personal financial information by financial institutions and companies who receive such information
  + **Safeguards** – financial institutions must develop, implement, and maintain comprehensive info security programs to protect data. Also applies to institutions such as CRAs that receive customer financial information
  + **Pretexting** - prohibits use of false pretenses, including fraud and impersonation, to obtain personal financial information such as bank balances. Also prohibits the knowing solicitation of pretexting
* Privacy protecting financial info that is not public; institutions may share nonpublic personal info w/ affiliates
  + (1) Must provide notice to customer through reasonable means such as direct mail (long, expensive, and complicated)
    - Consumer v. Customer - important distinction because only customer is entitled to automatic privacy notice
      * Consumer is an individual who obtains or has obtained product or service from financial institution - only entitled when financial institution shares info with non-exempt 3rd parties
      * Customer has continuing relationship with institution
    - Notice must be clear and accurate statement of company privacy practices including what it collects and whom it shares it with
  + (2) Opt-Out Rights - right to opt out of having information shared with *certain* 3rd parties and duty for institution to provide reasonable way of doing so
    - Does not apply to disclosures to credit reporting agencies, affiliates, outside companies that provide essential services (e.g. data processing), or marketers of the financial institutions products/services
    - Share financial info w/ non-affiliates [very small category] w/ opt-out notice unless joint marketing deal
  + Cannot disclose account numbers of credit card numbers for use in direct marketing
* Requires the FTC and other agencies to establish security standards for nonpublic personal information. Financial institutions shall develop, implement, and maintain a comprehensive information security program that is appropriate to the size and complexity of the institution, the nature and scope of the institution’s activities, and the sensitivity of any customer information at issue
  + An information security program is defined as the administrative, technical, or physical safeguards an institution sues to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information
* Criticisms
  + Critics argue that the privacy notices under GLBA are difficult to understand and make it hard for consumers to opt out. This means that a lot of information can be shared.
  + Weak law in terms of consumer choice and poor notice; corporate influence driving info privacy policy
* Supporters argue that GLBA has required financial institutions to analyze their practices because they have to understand their own practices to provide the complex notices. This led many to change how they shared data as they didn’t like what they say.
  + Safeguards rule is also strong and it has the ability to preempt state laws to bring about uniformity

### *IRSG v. FTC* (2001 DC)

* Facts: TransUnion and industry association comprised of CRAs seek judicial review and challenge regulations promulgated by agencies to enforce GLB. They argue regulation of credit header information will be affected by the regulations and thus have standing
* Holding - new rules are lawful and constitutional
  + Personally identifiable financial information is an ambiguous term and the agency interpretation is entitled to deference. It rejects ISRG argument that definition in new regulations were too broad
  + Language and legislative history suggest reuse and re-disclosure limitations are implicit in the statute. While can disclose to CRA's without opt-out, this doesn't apply to further use or disclosure by CRA
  + 1A argument fails - this is commercial speech which is subject to lesser protections. It is not related to any matter of public concern
  + The new rules do not directly prohibit the use and disclosure of nonpublic personal information, but instead require financial institutions to provide customers with notice and the opportunity to opt out. This is **consistent with the purpose of GLA - to allow consumers to retain control over their financial information** - and thus it can't be said that the government interest here is too small to justify such broad use restrictions, even in light of the significant effects it would have on the use of credit-header products
* Key takeaway - Shows the indirect impact on databroker and marketing industry

### *Guin v. Brazos* (2006 MN)

* Facts: Telecommuter with unencrypted laptop has the device stolen from their home. Laptop hardrive contained files which included personal financial information. P brings negligence suit, arguing GLBA established duty
* Holding:
  + In order to prevail, must show existence of duty, breach, and harm
  + GLB requires comprehension information security program. Hoewver, court concludes there is insufficient evidence from which fact finder could determine D failed to comply with GLB
    - GLB does not establish requirement to encrypt or prohibit working on sensitive data in their homes
    - Since no breach of a legal duty, no liability for negligence
  + Further, even if there were a breach, P failed to show that any harm occurred as a result. No evidence was presented that those who burlarized laptop targeted the personal data of P

### *Huggins v. Citibank* (2003 SC)

* Facts: P sued several banks, contending that they negligently issued credit cards to an unknown imposter, John Doe, who applied for the cards asserting that he was P. The cards were used to incur large amounts of debt. P contends Banks were negligent for failing to investigate or verify Doe's identity before issuing the cards and for the grief that he suffered when creditors tried to collect the debt
* Holding: Banks not liable under negligence theory
  + Tort of negligence requires P establish that there was some duty of care/harm prevention that D owed to P. Here, the relationship between the credit card issuers and P were insufficient to establish such a duty
  + While court expresses concern about identity theft and acknowledges that increased scrutiny in the credit application process would certainly reduce identity theft, the relationship is too attenuated and would thus extend tort liability beyond reasonable limits if D was held liable

### Criminal Liability for Identity Theft or Violating Financial Privacy

* GLBA's Pretexting Provisions
  + Using false statements or documents to obtain information from financial institutions or individuals
* Identity Theft Assumption and Deterrence Act
  + Knowingly using a means of identification with the intent to commit any unlawful activity or felony under state or federal law
* Computer Fraud and Abuse Act
  + Knowingly accessing a computer without authorization
  + Intentionally accessing a protected computer without authorization and as a result of such conduct recklessly causes damage
  + Theft of property via computer
  + Trafficking in passwords (e.g. via phishing)

## Online Privacy

### Children’s Online Privacy Protection Act (COPPA - 1998)

* Regulates the collection and use of information from children under age 13 by Internet sites
  + Website must target children or have actual knowledge that it is collecting personal information from another site/service directed at children
    - Will consider its subject matter, visual content, or other characteristics in determining whether targeted at children
* Collection: (1) requesting or prompting child to submit personal information; (2) enabling child to make personal information publically available in a personally identifiable form; or (3) passive tracking of child online
* Personal info and PII: voice/audio/image files; geolocation data; online contact info; persistent identifiers
* Must have privacy policies providing notice of collection, use and disclosure of information
* Consent: obtain verifiable parental consent to collect, use, or disclosure children’s information. How to get consent (this is where datedness shows)?
  + Paper consent and snail mail
  + Use of credit card with transaction log
  + Toll free number or video conference with trained personnel
  + Check government ID
  + If there is no disclosure, then "email plus" will suffice
* Liability: hosts liable for 3rd party activities on sites when 3rd parties have actual knowledge
* Enforcement: Fines up to $16k per violation; no private cause of action
* Preemption of all state law
* Safe Harbor: Following self-regulatory guidelines from marketing or online industry groups approved by FTC

### Online Behavioral Advertising

* OBA consists of the collection of data online from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites to predict user preferences or interests or to deliver advertising to that computer/device based on prefences of interests inferred from such Web viewing behavior
* Transparency and consumer control
  + Opportunity to exercise choices will "never be more than a few clicks away" from standardized wording and link/icon
  + Ad choices page to allow user to control/opt-out over ad preferences
* No federal statute squarely occupying space
  + GDPR has had extra-territorial impact since it took effect in 2018
* Example of self-regulation as an approach to privacy law and policy
  + Industry writes and enforces rules and guidelines

## Cloud and IoT

* IoT ("Internet of Things") refers to the ability of evereday objects to connect to the internet and to send and receive data
  + Experts estimate that there will be 50 billion such connected devices by the year 2020
  + Real time monitoring of information collected by these devices offers tremendous benefits (e.g. health care, energy use, road safety)
  + However, presents great security risks including:
    1. Enabling unauthroized access and misuse of personal information collected by these devices
    2. Facilitating attacks on other systems (e.g. botnets)
    3. Creating risks to safety by altering the physical behavior of these connected devices
  + Also unique privacy risks, including:
    1. Sensitive personal information (e.g. precise geolocation, health vitals, and financial account numbers) is being directly collected, often without consumer awareness or meaningful consent
    2. Infrences that can be made about personal habits and physical conditions (e.g. health and mental condtion, lifetyle, mood) based on the sheer volume and nature of information collected. The amount and granularity of data allows analyses to be performed that wouldn't otherwise be possible. This runs the risk of this information being used in unauthorized ways and having real-world consequences (e.g. employment, credit access, health insurace costs)
       - FCRA imposes obligations on CRAs, but excludes most "first parties" that collect consumer information and would not cover device manufacturers that perform the collection/analytics themselves. Thus, would not cover companies that collect data directly and use them to make in-house credit/insurance eligibility decisions

# Emerging Privacy Frameworks

## GDPR

* General Data Protection Regulation (GDPR) is a significant update to Europe's comprehensive privacy law. The GDPR became applicable on May 25, 2018
  + Strengthens data protection under law, providing new data protection rights to individuals and responsibilities for entities handling personal data

### GDPR Overview

* **Chapter 1: General Provisions**
  + GDPR generally applies when **personal data** of a data subject is processed
    - Personal data is information that can identify an individual (including some pseudonymized data if it can be linked back to an individual, but not fully anonymous data)
    - Certain sensitive data, like biometrics, warrant heightened protection
  + **Processing** is broadly defined and includes may types of activities related to handling data, like collection, transmission, and storage
  + GDPR applies to **controllers**, those who direct the purposes and means of how data is processed, and **processors**, those that actually process the data on behalf of the controller
  + GDPR applies to both the public and private sectors (national security/law enforcement exception. It also applies to **all companies which process European consumers' personal data**. This includes:
    - Companies with an “establishment” in the EU, regardless of where they process personal data. This would mean cloud-based processing performed outside of the EU for an EU-based company is covered
    - Companies that monitor behavior and collect data on subjects who are located within the EU (even if no transactions take place). Generally, these companies will need to appoint a representative in the EU
    - Companies based outside the EU that provide services or goods to the EU (including for free). These companies may also need to appoint representative in the EU
* **Chapter 2: Principles**
  + General Principles for Processing Data - Data must be:
    - Processed lawfully, fairly and in a transparent manner in relation to individuals
    - Collected for specified, explicit and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes (unless public interest exception)
    - Adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed
    - Accurate and, where necessary, kept up to date; Reasonable steps taken to
    - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
    - Processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss
  + Lawfulness of processing One of six lawful bases for processing must be present before any processing can occur:
    - Consent of the data subject - Made by clear **affirmative action** (opt-in)
    - Contract
    - Legal obligation
    - Vital interests
    - Public interest
    - Legitimate interests - Where processing is necessary for the legitimate interests of the controller, except where overridden by the interests or fundamental rights and freedoms of the data subject)
* **Chapter 3: Rights of the Data Subject**
  + The right to be informed - When their data is collected, data subjects must be informed about the purposes for which the data will be processed, the categories of personal data obtained, how long it will be retained, and more
  + The right of access - Right to information about whether their data is being processed, and, if so, have a right to access their personal data which is being processed
  + The right to rectification - Right to correct their personal data or complete any data which is incomplete
  + The right to erasure - Right to erasure of personal data which has been collected (i.e. a right to be forgotten) in certain circumstances, including that the data is no longer necessary for the purposes it was collected
  + The right to restrict processing - Right to request that an entity limit the processing of his or her data in certain circumstances, for instance where the individual alleges the data is incorrect or is being unlawfully processed
  + The right to data portability - Right to obtain their data from a service and transmit it to another service for use
  + The right to object - Data subjects have a right to object to processing based on "legitimate interest", to direct marketing, and to processing for research purposes
  + Rights related to automated decision making and profiling - Special heightened rights when they are profiled or evaluated by some automated process or algorithm, including the right not to be subject to them where it has legal or similarly significant effects or the right to know that they are subject to one
    - Exceptions to data subject's ability to object: Necessary for performing a contract between controller; Authorized by EU or Member state law; Is based on explicit (opt-in) consent; Legitimate grounds that override rights of data subject/legal claims
* **Chapter 4 : Obligations of Controller and Processor**
  + Data protection by design and by default - Technical and organizational measures must be implemented to advance data protection principles
  + EU representative - Entities outside the EU but subject to the GDPR must have a representative in the EU
  + Record-keeping - Records of processing activities must be kept
  + Security of processing - Technical and organizational measures must be implemented to ensure security, like pseudonymization and encryption
  + Notification of data breach - Within 72 hours of becoming aware of a data breach that poses a risk to individual rights and freedoms, a supervisory authority must be notified. Data subjects must be notified without undue delay
  + Data protection impact assessments (DPIAs) - An assessment of the risks to data protection is required processing runs a high risk for individual rights, and must consult a supervisory authority before processing where the DPIA indicates a high risk is no protective measures are taken
  + Data protection officers - DPOs must be appointed to oversee and advise on compliance issues if the entity is a public authorities, or an entity with core activities involving large scale, regular and systematic monitoring of individuals or large scale processing of special categories of data or data concerning criminal convictions and offenses
* **Chapter 5: Transfers of personal data to third countries or international orgs**
  + The transfer of personal data outside the EU is limited unless data protection guarantees under the GDPR will be maintained - such as where commission decides country adequate protections/safeguards and contractual
  + Commission takes into account a number of considerations in assessing the adequacy of the level of protection, including: the country's legislation, respect for freedoms, national security measures, etc
  + In the absence of an adequacy determination, a controller or processor may transfer personal data to a third country **only if** the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (usually via contract)
* **Chapter 6: Independent supervisory authorities**
  + Each member state must provide independent supervisory authorities that monitor and enforce GDPR (e.g. through fines, investigations, orders, guidance, etc.). Purpose of this is consistent application of GDPR throughout the EU
* **Chapter 7: Cooperation and consistency**
  + Establishes a system of coordination, information sharing, and assistance between aforementioned supervisory authorities. Creates a consistency mechanism to ensure common approach to enforcement of GDPR. Also establishes a European Data Protection Board, an official body of the EU that will resolve disputes between authorities and work to adopt new guidelines and recommendations
* **Chapter 8: Remedies, liability and penalties**
  + Individuals have the right to lodge complaints with a supervisory authority and a right to challenge in court an authority's legally binding decision concerning them
* **Chapter 9: Provisions relating to specific processing situations**
  + Sets out special standards for specific processing situations, such as how to reconcile protection of personal data with values like transparency, public access, and freedom of expression. This chapter permits (and sometimes requires) member states to set separate rules and conditions for certain specific contexts
* **Chapter 10: Delegated acts and implementing acts**
  + Authorizes European Commission to adopt delegated acts further developing and implementing the GDPR provisions
* **Chapter 11: Final Provisions**
  + Repeals the previous data protection directive and sets date of GDPR's applicability

### Key Changes from the EU Data Protection Directive

* Data processors as well as data controllers are directly liable under GDPR. Under the 1995 Directive, only controllers were directly liable. Data processors are now required to have a contract with data controllers to process personal data
* Slightly expands definition of personal data, which is defined as "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier (e.g. name, uuid, IP, location,)...or to one or more factors specific to the...identity of that person". Under the Directive, personal data was defined as data such as names, photos, email addresses, phone numbers, addresses, and personal identification numbers (social security, bank account, etc.)
* Two new categories of data, genetic and biometric data, join the prior list of “sensitive” or “special” personal data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life and sexual orientation
* Under GDPR, organizations must delete data that is not being used for its original purpose
* Heightened consent requirements. GDPR requires explicit opt-in for the processing of any personal data, and **consent for the use of personal data must be informed, specific, and unambiguous**. Thus, now require clear affirmative action, and individuals can revoke their consent to data processing at any time. Consumers also cannot be asked to agree to contract terms in exchange for their consent
* New rights established
  + Right to access - Gives individuals the right to obtain from data controllers information on how their data is being used, where, and for what purpose. Also entitled to copy of information stored on them, free of charge
  + Right to be forgotten - if a person submits such a request, data controllers must erase and cease all further use of the data
* Along with new documentation requirements, organizations are now required to actively track how and where data is stored and used throughout the supply chain. This entails adopting risk management tools, building security and privacy into their operations by design, and conducting impact assessments on certain activities
* Imposes single uniform breach notification law. Under the Directive, member states were free to adopt their own. Under GDPR controllers must notify their supervisory authority and individuals affected by a personal data breach within 72 hours of learning about the breach and must provide certain details in the notification
* Penalties - For some GDPR violations, such as lacking consent to process data or violating privacy by design, organizations could be charged up to 4% of their global revenue. Other violations such as failing to keep records could see fines up to 2%
* The territorial scope has been increased. The regulation applies to all companies that process personal data of people residing in the EU, regardless of the company’s location
* Other Changes - The minimum age for individuals whose data can be collected rises from 13 to 16. Large data controllers must appoint a data protection officer. There is a single national office for complaints

### CCPA

* Differences From GDPR
  + Small firm exemption
  + Incl. of firms controlled by covered firms
  + Inclusion of households and devices
  + Omission of pseudonymous data
  + No right of correction
  + Opt out instead of opt in
  + No ability to limit processing
  + Bundling of consent
  + 12-mo. limit on consent
  + Time limits on data retention
  + Smaller penalties(?)
  + Fewer institutional obligations

## Cases Under Arising out of the EU Data Protection Directive of 1995

### *Bodil Lindqvist v. Jönköping* (ECJ, 2003)

* Facts: D set up a site for her church with information about her and other staff members of her parish. Information included their full names, telephone numbers, and family circumstances. However, D did not inform her colleagues or the proper authorities. She was charged with violating the Swedish data protection law that was passed to satisfy the 1995 Directive
* Holding: ECJ addresses several questions regarding the interpretation of the Swedish law and the 1995 Directive
  + The act of referring, on an internet page, to persons and identifying them by name or by other means constitutes the "processing of personal data wholly or partly by automatic means" under the meaning of the Directive. Thus, D's failure to notify subjects prior to this "processing" was a violation
    - Names are clearly information relating to an identifiable person, and loading personal data on an internet page is processing that information
  + Reference to the fact that one of the staff members injured their foot and was on medical leave constitutes sensitive data concerning health for the purpose of the Directive. Processing this information without prior authorization violated the law
  + There was no transfer of data to a third country, within the meaning of the directive, where an individual loads personal data onto an internet page which is hosted within an EU member state, but accessible by anyone who connects to the internet (including those people in a third country)
    - The alternative construction would to be too broad of a reading. People could never share information online since many countries with access to the internet lack the privacy protections of the EU. Thus, D’s sharing of information online did not constitute a transfer of data to a third country
  + Finally , Directive does not conflict with freedom of expression and other freedoms because it is the obligation of national authorities, in implementing the directive through its own legislation. to ensure a fair balance between the rights and interests in question. Any such infringements on freedoms are the result of the member state's implementation, not the directive itself

### *College van burgemeester en wethouders van Rotterdam v. Rijkeboer* (ECJ 2009)

* Background: Case concerning individual's right, under the 1995 Directive, of access to data and information on the sharing of that data. Rijkeboer, P, brought suit against the College after it declined to fully provide him information on the disclosure of his personal data to third parties over the last three years. The College, however, had partially complied with his request by providing such information, but only that which dated back to the previous year. The College argues that the Directive does not provide any fixed time period and that it had complied with the law of the Netherlands (which only requires 1-year history)
* Holding:
  + Court holds the Directive clearly requires Member States to ensure a right of access to information on the recipients of personal data and on the content of that data, not only in respect of the present but also in respect of the past. However, the court says it is for Member States to fix a time-limit for storage and access to that information which constitutes a fair and reasonable balance between privacy interests of the individual and the burden it would impose on the controller
  + Asserts limiting the storage of this information to a period of one year, while basic data is stored for a much longer period, **do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller**
    - However, ECJ says it is up to the for the national courts (of the Netherlands) to make this determination about the burden such expanded retention periods would have on data controllers

### *Heniz Huber v. Germany* (ECJ 2008)

* Facts: Huber, an Austrian national, moved to Germany in 1996 in order to work there as a self-employed insurance agent. The following data was stored in the German Central Register of Foreign Nationals: his name, date and place of birth, nationality, marital status and gender; a record of his entries into and exits from Germany, and his residence status; details of passports issued to him; a record of his previous domicile; and reference numbers issued by the Bundesamt (Office for Migration). Huber claimed he was discriminated against because no such database existed in respect of German nationals and unsuccessfully moved to have this data erased
* Holding:
  + ECJ rules that a system for processing personal data relating to EU citizens, who are not nationals of the Member State concerned, and intended to support to the national immigration authorities, does not satisfy the requirement of necessity as an exception to the prohibition on any discrimination on grounds of nationality, unless:
    - It contains only the data which are necessary for the application by those authorities, and
    - Its centralized nature enables the legislation relating to the right of residence (i.e. immigration law) to be more effectively applied as regards EU citizens who are not nationals of that Member State
  + It is up to the national courts of Germany to determine whether such criteria are met
    - The storage and processing of individualized personal information for statistical purposes cannot, for example, could not be considered as necessary under this meaning

## The Safe Harbor Arrangement

* 1995 DPD regulated transfer of personal data to third countries with the following principles:
  + Transfer may take place only if the third country in question can ensure adequate levels of protection
    - Adequate protection does not mean equivalent protection. Shall be assessed in light of the circumstances surrounding the transfer, the nature of the data, proposed use/processing, the rules of law of the of the country, and its professional rules, standards, and security measures
  + Member states must information each other in cases where they determine the third country cannot ensure such adequate protection. Member state must then take measures necessary to avoid all such future transfers of the same nature to that third country
* Major differences between the EU privacy directive and the US approach
  + US also lacks omnibus privacy protection law
  + Threatens the free flow of information between the two
  + Also leaves American as second class citizens in the global market as many areas adopting the EU approach and its heightened privacy
* To preserve the billions of dollars in trade and data flows of US based MNCs operating in the EU, the US and EU successfully negotiated a "Safe Harbor" arrangement in 2000
  + Designed to protect privacy of EU citizens without forcing the US to adopt EU style privacy rules
  + Under the agreement, US firms may transfer data if they participate in self-certification/regulatory privacy program that conforms to the Safe Harbor (e.g. TRUSTe)
* Certifying firms are expected to adopt a published privacy policy and adhere to the seven Safe Harbor principles:
  + **Notice**: an organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses information, and the choices and means the organization offers individuals for limiting its use and disclosure
    - Notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information
  + **Choice**: an organization must offer individuals the opportunity to choose (opt out) whether their personal information is
    - To be disclosed to a third party or
    - To be used for a purpose incompatible with the purpose for which it was collected
      * If information sensitive (e.g. medical information, race, etc.), then must opt in
  + **Access**: individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate
  + **Onward transfer**: to disclose information to third parties, organizations must follow the notice and choice principles. Must ensure that the third party is following the same stringent privacy standards
  + **Security**: must protect personal information
  + **Data integrity**: personal information must be relevant for the purposes for which it is to be used
    - An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current
  + **Enforcement**: effective privacy protection must include mechanisms to assure compliance with the principles

## Right to Be Forgotten

### *Google Spain v. AEPD* (2014 ECJ)

* Facts: Complaint based on fact that a Google search linked two newspaper old articles to a man’s name. Article pertained to 16 year old data about real-estate auction connected with attachment proceedings for recovery of social security debt
* Holding: Links must be removed from the list of results
* Reasoning:
  + Uploading information to internet is processing personal data. Thus, search engine engages in processing personal data when it searches and collects such information
    - This makes search engine operator a controller of personal data
  + Court concerned about ability to use a name to get a list of information on a person through a search engine, especially when it is likely personal
    - Needs to be a balance between privacy interests and the interest in having readily available information. Usually privacy interests outweigh accessibility, but may not be the case when great public interest in having the information or when the cost of removing would be particularly burdensome on the processor
    - Here, privacy is given more weight. Some exceptions, such as if person a public figure and interest in their life. Basically needs to be an overriding public interest in that information. However, such public interest is not served here and thus privacy prevails
  + Person may request information be removed from search results, even if true and not prejudicial, and the search engine must erase it
* Notes
  + Establishes that the operator of a search engine is a processor of data under the Directive and could not simply justify its activity through economic interest in processing and it was not protected by language regarding journalism
    - Further, even when the publication of information may have been lawful, the operator could still be required to remove the person’s name from search results
  + Court also found that a person has a strong interest in the right to be forgotten, which often outweighs the economic interest of the operator in running the search engine and the interest of the public in having access to the information
  + Ability to have keep information on the web almost indefinitely a problem. However, the decision poorly addresses it because it only talked about removing links to personal information. Didn’t address requiring information to be removed from the web entirely
  + Responding to the decision, Google set up a web page allowing people to request search removal. Stated that it would balance the rights of the individual against the public’s interest to know and the right to distribute information. Would look at whether the information was outdated and whether there was a public interest in it
* Related Proceedings
  + Highest German court says Google Autocomplete can violate personality rights because it reflects search activity of users and content of web pages; software generates untrue statements of fact
  + Not really about the right to be forgotten because web site still exists
  + The goal is to keep individuals from forming an initial opinion with prejudicing info

### *IMS v. Sorrell* (SCOTUS – 2011)

* Facts:
  + Vermont law restricts sale, disclosure, and use of pharmacy records that reveal prescribing practices of individual doctors
  + Vermont argues that its prohibitions safeguard medical privacy and diminish the likelihood that marketing will lead to prescription decisions not in the best interest of the patients or the state
  + Issue of free speech in marketing also comes in
  + Case brought by 3 Vermont data miners and an association of pharma manufacturers that produce brand name goods
* Rule: **Prescriber-identifying info is speech for 1A purposes since facts marking beginning point of speech essential for advancement of human knowledge**
* Holding:
  + State cannot engage in content-based discrimination to advance its own side of the debate
  + Privacy is a concept too integral to the person and a right too essential to freedom to allow
  + State “burdened” a form of protected expression that it found “too persuasive” – but the court cannot do this (so the law is unconstitutional)
* Dissent (Breyer):
  + The law is constitutional as the only type of expression being regulated is means of data collection aimed to benefit pharma sales

### GDPR Article 17 - Erasure (Right to Be Forgotten)

* Data subject can request erasure of personal data when:
  + Personal data are no longer necessary
  + Consent is withdrawn
  + Data subject objects and there are no legitimate grounds
  + Processing has been unlawful
  + Erasure is for compliance with legal obligation
* Guidance from Data Protection Board
* Right shall not apply if processing is necessary for:
  + Right of freedom of expression and information
  + Compliance with legal obligation or task in the public interest or in the official authority vested in the controller
  + Reasons of public interest in area of public health
  + Archiving for pub. int., sci., hist. research, stat. purposes
  + Establishment, exercise or defense of legal claims
* Guidance from Data Protection Board
  + Blacklisting/Early Warning Systems and Asset Freezing

### American vs. European Conceptions of Privacy

* **American**
  + Primarily concerned with protection of the home; little focus on media
  + Sovereignty within our own walls
  + Most concerned with deprivations of liberty by the state
  + Home is primary defense and state is primary enemy
  + State action is the biggest issue
* **European**
  + Common to maintain a fundamental right to privacy
  + Continental law of privacy protects dignity and honor broadly
  + Europeans concerned w/ display of consideration for public dignity
  + Historical legacy of Fascism and monarchical societies led to desire for personal honor/dignity