Medical Privacy

Confidentiality of Substance Use Disorder Patient Records Rule

- Does not preempt stricter state laws
- **Scope:** covers the disclosure of "patient identifying" information by treatment programs for alcohol and substance abuse.
- **Applicability:** any program that receives federal funding:
    - Individual or entity that provides alcohol or substance abuse diagnosis, treatment, referral for treatment
    - An identified unit within a general medical facility that provides alcohol or substance abuse diagnosis, treatment, referral for treatment
    - Medical personnel or other staff in a general medical facility who primary function is the provision of alcohol or substance abuse diagnosis, treatment, referral for treatment.
- **Disclosure:** must obtain written patient consent before disclosing
- **Redisclosure:** prohibited when that information would "identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment."
- **Exceptions to consent requirements:**
    - Medical emergencies
    - Scientific Research
    - Audits and evals
    - Communications with a qualified service organization
    - Crimes on program premise or against personnel
    - Child abuse reporting
    - Court order
- **Violations:** First one not more than $500. $5000 for each subsequent offense. Reported to U.S Attorney's Office

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Updated by Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
- Regulated by the Department of Health and Human Services (HHS)
- Does not preempt stricter state privacy laws (Ex: California Medical Information Privacy Act)
- No private right of action
- FERPA applies to student health records. HIPAA applies to non-student health records.
- **Applicability**: "covered entities," healthcare providers, insurers, business associates
    - Healthcare providers: doctors' offices, hospitals
    - Health plans (health insurers)
    - Healthcare clearinghouses
    - Business associates (Ex: PHI stored on the cloud)
- **The Privacy Rule:**
    - **Privacy Notice:** must provide notice at date of first service delivery and must describe rights to individual's PHI

  - **Authorization for uses and disclosures:** PHI use and disclosure for treatment, payment, and operations (TPO). Other uses require individual to opt-in.
  - **Minimum Necessary use or disclosure:** covered entities must limit use and disclosure to minimum necessary. Business associates must be bound by this standard.
  - **Access and accountings of disclosures:** Individuals have the right to access and copy their own PHI. Individuals have the right to amend PHI, and if denied, individual may file a statement that must then be included in any future use or disclosure of info.
  - **Safeguards:** covered entities and business associated must implement administrative, physical and technical safeguards to protect confidentiality and integrity of PHI and ePHI.
  - **Accountability:** entities must designate privacy official and personnel must be trained. Must have complaint procedures in place.
  - **Enforcement:** Office of Civil Rights (OCR). U.S Department of Justice (DOJ) has criminal enforcement authority (prison sentences up to 10 years). FTC can enforce under section 5 "unfair and deceptive practices." State AGs.
  - **Exceptions:**
    - **De-identified data:** 1. Remove at least 17 data elements 2. Have an expert certify
    - **Research:** permitted on de-identified data
    - **Other:** public health activities, report victim of abuse, neglect, or domestic violence, judicial and administrative proceedings, certain law enforcement activities, specialized government functions. Must release to individual and HHS.
- **The Security Rule:** minimum security requirements for PHI that a covered entity receives, creates, maintains or transmits in electronic form.
  - Ensure confidentiality, integrity, and availability of all ePHI
  - Protect against any reasonably anticipated threats to ePHI
  - Protect against any reasonably anticipated disclosures of ePHI
  - Ensure compliance with the Security Rule by its workforce
  - Each covered entity must have individual responsible for oversight and implementation
  - Covered entity must conduct initial and ongoing risk assessments
  - Covered entity must implement security awareness and training program for workforce
- Qualified Protective Order (QPO) prohibits litigating parties from using or disclosing the protected health info for any purpose other than the litigation or proceeding for which such info was requested. It also requires the return to the covered entity or destruction of PHI (including copies) at the end of litigation.
- Disclosure under HIPAA pursuant to a court order or subpoena is permitted if three criteria are met:
  - The info sought is relevant and material to legit law enforcement inquiry
  - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the info is sought
  - De-identified info could not be reasonably used
- Permits disclosure of PHI to authorized federal officials for the conduct of lawful intelligence, counter intelligence, and other national security under the National Security Act.

The Health Information Technology for Economic and Clinical Health Act (HITECH)

- Strengthened HIPAA to address privacy impacts of the expanded use of electronic health records
- **Breach:** must notify individuals within 60 days of discovery
    - If more than 500 people, must notify HHS immediately
    - If 500 or more in the same jurisdiction, must notify media
    - Covered entity can avoid liability if they utilize encryption software
- **Penalties:** up to $1.5 mil for most willful violations
- **Disclosure:** Must be minimum amount necessary
- Covered entities may not sell Electronic Health Records (EHR) without the consent of the patient

Genetic Information Nondiscrimination Act of 2008 (GINA)

- Created new national limits on the use of genetic information in health insurance and employment
- Prohibits employers from requiring, requesting, or purchasing such genetic information about employees or family members except:
    - Such a request if inadvertent
    - Request is part of an employer-wellness program and voluntary
    - Request is made to comply with the Family and Medical Leave Act (FMLA)
    - Employer purchases commercially and publicly available info
    - The information is used for legally required genetic monitoring for toxin exposure in the workplace and employee voluntarily participates with written consent
    - Employer conducts DNA analysis for law enforcement and quality control purposes.
- If employer possesses info, it must be kept in a separate form separate from medical files
- No private right to action -but private rights of action may be available under the federal laws that GINA revises as well as under similar state laws.
- **Amended:** Employee Retirement Income Security Act (ERISA), the Social Security Act, and the Civil Rights Act.
- **Penalties:** $100/day of noncompliance. Minimum can rise to $15,000

The 21st Century Cures Act of 2016 (Cures Act)

- Expedite the research process for new medical devices and prescription drug, quicken process for drug approval, reform mental health treatment
- **Privacy Provisions:**
    - Certain individual biomedical research information exempted from disclosure under FOIA
    - Researchers permitted to remotely view PHI (must meet minimum safeguards consistent with HIPAA's Privacy and Security Rules)
    - Information blocking prohibited but HIPAA's protection of PHI remains

- Certificates of confidentiality for research. Must be issued by NIH for any federally funded research. Research material cannot be used in any legal or administrative proceedings without patient's consent.
- Compassionate sharing of mental health or substance abuse information with family or caregivers

Financial Privacy

The Fair Credit Reporting Act (FCRA)

- Mandates accurate and relevant data collection, provides consumers with the ability to access and correct their information, and limits the use of consumer reports to defined permissible purposes.
- Regulates use of consumer reports obtained from CRAs in reference checking and background checks of employees
- Generally, preempts state law (see FACTA)
  - Does not preempt states from creating stronger legislation in the area of employment credit history checks such as the California ICRAA
- **Enforcement:** dispute resolution, private litigation (private right to action), government actions (FTC, CFPB, State AGs)
- **Violations:** civil/criminal penalties. Statutory damages of at least $1000 per violation, and at least $3,756 for willful violations.
- Amended by FACTA with provisions related to identity theft and other subjects
- Regulates any consumer reporting agency
  - **Consumer report is any communication by a CRA that pertains to:**
    - Creditworthiness
    - Credit Standing
    - Credit Capacity
    - Character
    - General Reputation
    - Personal Characteristics
    - Mode of Living
  - **Users of consumer reports must meet:**
    - Third party data for decision making must be accurate, current, and complete
    - Consumers must receive notice when third party data is used to make adverse decisions
    - May only be used for permissible purposes
    - Consumers must have access to their consumer reports and an opportunity to dispute or correct errors
  - **CRA's MUST:**

- Provide consumers with access to info in report and the opportunity to dispute/correct errors
- Ensure maximum possible accuracy of report
- Not report negative info that is outdated (account data more than seven years old, bankruptcies older than 10 years)
- Provide reports only to entities that have permissible purpose
- Maintain records regarding entities that received reports
- Provide consumer assistance as required by FTC

- **Notice Provided by CRA's To Users:**
  - Users must have a "permissible purpose"
    - Court order
    - Instructed by consumer in writing
    - Extension of credit as a result of application by consumer
    - Employment purposes where consumer has given written consent
    - Underwriting of insurance initiated by consumer
    - To review consumer's account to determine if account needs are met
    - Determine consumer's eligibility for license or other benefit granted by government
    - For use by potential investor/servicer/current insurer in a valuation assessment
    - For use by state and local officials in connection with child support payments
    - Creditors and insurers may obtain certain consumer report info for the purpose of making prescreened unsolicited offers of credit or insurance
  - Users must provide certifications of permissible purpose
  - Users must notify consumers when adverse actions are taken and must include:
    - Name, address, telephone number of the CRA
    - Statement that the CRA did not make the adverse action and cannot explain why it was made
    - Statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days
    - Statement setting forth consumer's right to dispute directly with the CRA the accuracy and completeness of any info provided by CRA

        - Adverse Action based on non-CRA: must inform consumer their right to be informed of the nature of the info that was relied upon if request is made within 60 days of notification.
        - Adverse Action based on affiliates: must inform consumer that they may obtain disclosure of the nature of the info relied upon by making a written request within 60 days of notification. The user must disclose no later than 30 days after receiving the request.
- Companies that extend credit to consumers must implement "Red Flag" program to deter identity theft
- Employee investigation not treated as a consumer report as long as:
    - The employer or its agent complies with the procedures set forth in FCRA
    - No credit info is used
    - A summary describing the nature and scope of the inquiry is provided to the employee if an adverse action is taken
- **Consumer rights for investigative consumer reports:**
    - Consumer must be informed than investigative consumer report may be obtained
    - Disclosure must be in writing and delivered to consumer some time before but not later than three days after the date which the report was first requested
    - Disclosure must include a statement informing the consumer of his or her right to request additional disclosures and a summary of consumer rights under FCRA
    - User must certify to the CRA that the required disclosures have been made
    - Upon written request of a consumer, the user must make a complete disclosure of the nature and scope of the investigation
    - Nature and scope disclosures must be made in a written statement that mailed or delivered to consumer no later than five days after the date on which the request was received from the consumer or the report was first requested (whichever later)
- Consumer must provide consent for any medical info to be used under FCRA
- Permissible purposes for employment checks include:
    - Pre-employee screening for the purpose of evaluating the candidate for employment
    - Determining if an existing employee qualifies for promotion, reassignment, or retention
- FCRA applies to nontraditional providers of background check information (like social media aggregators)

The Fair and Accurate Credit Transactions Act (FACTA)

- Made substantial amendments to FCRA
- CFPB is rule-making and enforcement authority
- Stricter state laws are preempted -states retain some powers to enact laws addressing identity theft
- Required truncation of debit and credit card numbers so receipts do not reveal in full

- Requires more detailed "know your customer" documentation for both domestic and foreign financial institutions.
- Gave consumers rights to explanation of their credit scores and the right to request a free annual credit report
- Promulgated Disposal Rule and Red Flags Rule
- **The Disposal Rule**
    - Requires any individual or entity that uses a consumer report, or information derived from a consumer report, for a business purpose to dispose of that information in a way that prevents unauthorized access and misuse of the data.
    - **Enforcement:** FTC, the federal banking regulators, and the CFPB
    - **Violations:** civil liability and may face federal and state enforcement actions
    - State disposal rules may impose broader requirements
- **The Red Flags Rule**
    - Requires certain financial entities to develop and implement written identity theft detection programs that can identify and respond to the "red flags" that signal identity theft.
    - The Red Flags Program Clarification Act of 2010 narrows the previously broad definition of creditor to not implicate entities that extend credit only for "expenses incidental to a service." Applies to:
        - Obtain or use of consumer reports in connection with a credit transaction
        - Furnish information to CRA
        - Advance funds to or on behalf of someone, except for expenses incidental to a service provided by the creditor to that person
    - Each entity is required to define their own list of red flags. FTC recommends:
        - Alerts from CRA
        - Suspicious identification documents
        - Suspicious personal identifying data
        - Unusual use of a covered account
    - FACTA provides that an employer is no longer required to notify an employee that it is obtaining an investigative consumer report on the employee from an outside org in the context of an internal investigation.
        - Changed the definition of consumer report under FCRA to exclude communications relating to employee investigations from the definition **if three requirements are met:**
            - Communication is made to an employer in connection with the investigation of:
                - Suspected misconduct relating to employment
                - Compliance with federal, state, local laws
            - Communication is not made for the purpose of investigating a consumer's creditworthiness, credit standing or credit capacity and does not include info pertaining to those factors
            - Communication is not provided to any person except
                - The employer or agent of employer
                - A federal or state officer, agency, or department

        - Self-regulating org with authority over the activities of the employer or employee
        - As otherwise required by law
        - Pursuant to 15 U.S.C 1681f which addresses disclosures to gov agencies
    - If adverse action is taken, employers must disclose a summary of the nature and substance of the communication or report to the employee

Gramm-Leach-Bliley Act (GLBA)

- Promulgated a Privacy Rule and Safeguards Rule. Sets the privacy framework for modern banking. Financial institutions must protect consumers' nonpublic personal info
- Stricter state laws are not preempted
- No private right to action, however, failure to comply with certain notice requirements may be considered a deceptive trade practice which some states give private right to action for.
- Under GLBA's privacy provisions, financial institutions are required to:
    - Store personal financial info in a secure manner
    - Provide notice of their policies regarding the sharing of personal financial info
    - Provide consumers with the choice to opt out of sharing some personal financial info
- Regulates financial institution management of "nonpublic personal information" defined as "personally identifiable financial information":
    - Provided by the consumer to a financial institution
    - Resulting from a transaction or service performed for the consumer or
    - Otherwise obtained by the financial institution
- Name of a financial institution's customer is considered non-public personal info and must be protected under GLBA
- **Enforcement:** federal financial regulators for institutions in their jurisdiction (Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Securities and Exchange Commissions). Financial institutions not in the jurisdiction of the other agencies (FTC and now also CFPB). At the state level, state AGs can enforce.
- **Violations:** subject to penalties under the Financial Institution Reform, Recovery, and Enforcement Act (FIRREA). FIRREA penalties range from up to $5,500 for violation of laws to a max of $27,500 if violations are unsafe, unsound, or reckless. $1mil for knowing violations.
- **Privacy Rule Components:** Financial institutions must:
    - Prepare and provide to customers clear and conspicuous notice of F.I's info sharing policies
    - Clearly provided customers the right to opt out of having their nonpublic personal info shared with nonaffiliated third parties (subject to exceptions such as joint marketing and transaction processing)
    - Refrain from disclosing to any nonaffiliated third-party marketer an account number or similar form of access code to a consumer's credit card, deposit or transaction account
    - Comply with regulations to protect the security and confidentiality of customer records and info. Protect against security threats and unauthorized access.
- **Privacy notices: must process opt outs within 30 days. Notice must contain:**
    - What info the F.I collects

    - With whom it shares the info
    - How it protects/safeguards the info
    - Explanation of opt out policy
- GLBA prohibits F.Is from disclosing info to nonaffiliated parties. F.I must ensure that service providers will not use provided consumer data for anything other than the intended purpose.
- Consumer cannot opt out if:
    - F.I shares info with outside company that provides crucial services like data processing
    - Disclosure is legally required
    - F.I shares customer data with outside service providers that market the financial company's products or services
- **The GLBA Safeguards Rule**
    - Requires F.I to maintain security controls to protect the confidentiality and integrity of personal consumer info, including both electronic and paper records.
    - F.I must develop an info sec program that addresses "administrative, technical, and physical safeguards."
    - Each F.I must:
        - Designate an employee to coordinate safeguards
        - Identify and assess risks to customer info
        - Design and implement a safeguard program and regularly monitor and test
        - Select appropriate service providers and enter into agreements with them
        - Evaluate and adjust the program in light of relevant circumstances
- Permits disclosure for an investigation on a matter related to public safety (National Security Act)

California Financial Information Privacy Act (California SB-1)

- Expands privacy protections afforded under GLBA and increases disclosure requirements of F.I's. Grants consumers rights with regards to info sharing.
- **Violations:** negligent noncompliance is punishable with statutory damages of $2,500 per consumer, up to $500,000/occurrence. Willful non-compliance eliminates the $500,000 cap.
- Must opt in for FI to share data with nonaffiliated parties
- Grants consumers opt out for info sharing between the FI and affiliates not in the same line of business

Dodd-Frank Wall Street Reform and Consumer Protection Act

- Created the CFPB as an independent bureau within the Federal Reserve
- CFPB can bring enforcement actions for unfairness and deception in addition to abusive acts and practices.
- **Enforcement authority of CFPB**
    - Ability to conduct investigations and issue subpoenas
    - Hold hearings and commence civil actions against offenders
- **Violations:** $5,526/day for federal consumer privacy law violations. $27,631/day for reckless violations. $1,105,241/day for knowing violations. State AG's can also bring civil actions in enforcement of law or regulations

The Bank Secrecy Act of 1970 (BSA)

- Aka "The Currency and Foreign Transaction Reporting Act" authorizes the U.S treasury secretary to issue regulations that impose extensive record-keeping and reporting requirements on F.I's
- Anti-money laundering and fraud effort
- F.I must keep records and file reports on certain financial transactions
    - currency transactions in excess of $10,000 (does not include credit secured by real property)
    - bank checks, drafts, cashier's checks, money orders, travelers checks for $3000 or more in currency
- **Applies to:** any entities subject to supervision by state or federal bank supervisory authority (banks, securities brokers, card clubs, etc)
- Certain funds transfer exempted from regulation including those governed by the Electronic Funds Transfer Act and those made through automated clearinghouses, ATM or point of sales systems.
- **Record Retention:**
    - Only those with "high degree of usefulness"
    - Must include:
        - Borrower's name and address
        - Credit amount
        - Purpose and date of credit
    - Such records may be maintained for five years
    - For deposit account records:
        - Depositor's taxpayer ID
        - Signature cards
        - Checks exceeding $100
- **Suspicious Activity Reports (SAR)**
    - FI must file in certain situations. Alerts gov to suspicious transactions
    - Must be filed with the U.S Department of Treasury's Financial Crimes Enforcement Network in the following circumstances:
        - When an FI suspects an insider committing a crime regardless of dollar amount
        - When entity detects crime involving $5000 and has substantial basis for identifying suspect
        - When entity detects crime involving $25000 (no need for suspect)
        - When entity detects currency transactions aggregating $5000 or more that involve potential money laundering
- **Violations:** civil penalties including fines up $25000 or the amount of the transaction (up to $100,000 max) as well as penalties for negligence ($500/violation). Additional penalties up to $5000 per day for failure to comply. Penalties up to $25000 for failure to comply with info sharing requirements of the USA PATRIOT Act. Penalties up to $1mil for failure to comply with due diligence requirements. Criminal penalties include up to $100,000 fine and/or 1 year imprisonment and up to $10,000 fine and or 5 year imprisonment.

The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001

- Part of the USA PATRIOT Act. Expanded the BSA reach. Gave U.S Treasury secretary the ability to promulgate broad rules to implement modified Know Your Customer requirements.

Education Privacy

Family Educational Rights and Privacy Act (FERPA)

- Provides students with control over disclosure and access to their educational records
- Applies to all educational institutions that receive federal funding
- No private right to action
- Mostly preempts state laws
- Provides students with the right to:
    - Control the disclosure of their education records to others
    - Review and seek amendment of their own education records
    - Receive annual notice of their rights under FERPA
    - File complaints with the U.S Department of Education
- Education Record: includes all records that are directly related to the student and maintained by the school or by a party on behalf of the school.
- Exceptions:
    - Campus police records
    - Employment records
    - Treatment records
    - Applicant records
    - Grades on peer-graded papers
- Disclosure is permitted only if one of the following conditions are met:
    - Info is not personal identifiable
    - Info is directory info whose release the student did not block
    - Consent provided by 1. The parent or 2. The student once 18 years
    - A statutory exception applies such as for health or safety purposes
- Personally Identifiable Info:
    - Student's name
    - Name of the student's parent or other family members
    - Student or student's family's address
    - Personal identifiers such as SSN or student number
    - Other identifiers such as D.O.B
    - Other info that alone or in combo would link to the student
    - Info requested by a person whom the school reasonably believes knows the identity of the student to which the education record is linked
- Directory info must have the option to opt out
- Valid student consent to disclosure must be signed and dated. Must also identify:
    - The record to be disclosed
    - The purpose of disclosure

    - To whom the disclosure is being made
- Disclosure Consent Exceptions:
    - Disclosure to school officials with "legitimate educational interest" in the records
    - Disclosure to education institutions which the student seeks or intends to enroll, or currently enrolled (transfers)
    - Disclosure in connection with financial aid that the student has received or which the student will apply for
    - Disclosure to orgs doing research studies for, or on behalf of, educational institutions
    - Disclosure to accrediting orgs
    - Disclosure to alleged victim of forcible or nonforcible sex offense
    - Disclosure of info related to sex offenders
    - Disclosure to a person or entity that is verified as the party that provided or created the record
    - Disclosure to law enforcement or otherwise to comply with a judicial order or subpoena
    - Disclosure to appropriate parties in connection with a health or safety emergency
- FERPA gives student right to access. School must provide records within 45 days of request
- If denied opportunity to fix a record, student must be given a hearing
- **Protection of Pupil Rights Amendment (PPRA)**
    - Applies to all elementary and secondary schools that receive federal funding. Postsecondary schools not included.
    - Provides certain rights to parents of minors with regard to the collection of sensitive info from students through surveys:
        - Political affiliation
        - Mental and psychological problems potentially embarrassing
        - Sex behavior and attitudes
        - Illegal, antisocial, self-incriminating and demeaning behavior
        - Critical appraisals of individuals
        - Legally recognized privileged relationships
        - Religious practices
        - Income (other than by law to determine program eligibility)

No Child Left Behind Act of 2001

- Broadened the PPRA to limit the collection of disclosure of student survey info. Now requires schools to:
    - Enact policies regarding the collection, disclosure or use of personal info about students for commercial purposes
    - Allow parents to access and inspect surveys and other commercial instruments before they are administered to the student
    - Provide advance notice to parents about the approx. date when these activities are scheduled
    - Provide parents the right to opt out of surveys or other sharing of student info for commercial purposes

Information Security and Breach Notification Privacy

California Assembly Bill 1950 (AB 1950) (first law)

- Encourage businesses that own or license personal info about Californians to provide reasonable security. Requires a business that owns or licenses personal info about a CA resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal info from unauthorized access, destruction, use, modification, or disclosure.
- Personal info:
    - An individual's name in combo with any one or more:
        - SSN
        - Driver's license number or CA id card number
        - Financial account number or cc or debit card number
        - Medical info
        - Health insurance info
        - Data collected from automated license plate recognition system
    - Personal info that is publicly available or encrypted is excluded
- Companies subject to HIPAA or GLBA are exempt

Massachusetts state security law 201 CMR 17.00 (most prescriptive)

- Establishes detailed minimum standards to safeguard person info contained in both paper and electronic records. Requires businesses holding personal info to:
    - Designate individual responsible for info sec
    - Anticipate risks to personal info and take appropriate steps to mitigate risks
    - Develop security program rules
    - Impose penalties for violations of the program rules
    - Prevent access to personal info by former employees
    - Contractually obligate third party service providers to maintain similar procedures
    - Restrict physical access to records containing PI
    - Monitor the effectiveness of the security program
    - Review the program at least once a year and whenever business changes could impact security
    - Document responses to incidents
- Mandates user authentication, access controls, encryption, monitoring, firewall protection, updates and training.

The Washington state security law House Bill 1149

- Part of the growing trend to incorporate the **payment card industry data security standard (PCI DSS)** into statute to ensure the security of credit card transactions and related personal info.
- Permits financial institutions to recover the costs associated with reissuance of credit and debit cards from large processors who negligence in the handling of credit card data is the proximate cause of the breach. Processors are not liable if the data were encrypted at the time of the breach or had been certified as PCI compliant within one year of the breach

Tennessee SB 2005

- Requires notice of breach regardless of whether information was encrypted or not
- 2017 amendment: the change clarified that encrypted data receives the protection of the safe harbor, unless the encryption key is also acquired in the breach

Illinois HB 1260

- added new protections for state residents and have more clearly defined what actions could result in public notification following a data breach.
- The changes expand the definition of protected personal information to include usernames and email addresses when combined with other information allowing a third party to access an individual's online account.
- Companies are required to alert affected parties to change their credentials if a combination of personal identifiers have been compromised.

California AB 2828

- A recently amended California state law now requires data breach notifications to be sent to residents when encrypted personal data has been breached
- California data breach notification law: requires notice that a breach occurred related to:
    - Both encrypted data and the encryption key or
    - Encrypted data when the business has a reasonable belief that the encryption key or security credentials can be obtained by the hacker

New Mexico HB 15

- Breach notification law
- The definition of “personal identifying information” includes biometric data, defined as an individual’s “fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual’s identity when the individual accesses a physical location, device, system or account.”
- The law applies to unencrypted computerized data or encrypted computerized data when the encryption key or code is also compromised.
- Notice to the New Mexico Office of the Attorney General and the major consumer reporting agencies is required if more than 1,000 New Mexico residents are notified.
- Notice must be made to New Mexico residents (and the Attorney General and Consumer Reporting agencies if over 1,000 residents are notified) within 45 calendar days of discovery of a security breach.
- Third-party service providers are also required to notify the data owner or licensor within 45 days of discovery of a data breach.
- Notice must be made to New Mexico residents (and the Attorney General and Consumer Reporting agencies if over 1,000 residents are notified) within 45 calendar days of discovery of a security breach.
- Third-party service providers are also required to notify the data owner or licensor within 45 days of discovery of a data breach.

Telemarketing and Marketing Privacy

The Telemarketing Sales Rule (TSR)

- Issued by the FTC in 1995
- FCC issued regulations under the **Telephone Consumer Protection Act of 1991 (TCPA)** that place restrictions on unsolicited advertising by phone and facsimile.
- Does not preempt stricter state laws
    - Some states require marketer obtain a license or register w/state
    - States can create their own DNC with differing exceptions/fines
    - Some states may require that a written contract be created for certain transactions
- May have private right to action via the intrusion on seclusion tort
- **Enforcement:** FTC, state AGs, or private individuals
- Defines telemarketing as a plan, program, or campaign which is conducted to induce the purchase of goods or services or charitable contribution, by use of one or more telephones and which involve more than one interstate telephone call
- Created the U.S National Do Not Call (DNC) Registry enforced by the FTC, FCC, and state AGs
    - Requires sellers and marketers to update their call lists every 31 days.
    - Exceptions to list:
        - Nonprofits calling on their own behalf
        - Calls to customers with existing business relationships (EBRs)
        - Inbound calls, provided there's no upsell of additional products/service
        - Most business to business calls
        - Consumer clearly and conspicuously opts in to calls
    - Telemarketers can avoid liability under the DNC safe harbor:
        - Seller/telemarketer established and implemented written procedures to honor consumers' requests
        - Seller/marketer has trained its personnel and any entity assisting in its compliance
        - Seller/telemarketer has maintained and recorded an entity specific DNC
        - Seller/telemarketer uses and maintains records documenting DNC and National DNC within 31 days of call
        - Seller/telemarketer monitors and enforces compliance with entity's DNC procedures
- **Violations:** civil penalties up to $40,654/call
- **TSR requires covered orgs to:**
    - Call only between 8am and 9pm
    - Screen and scrub names against national DNC list
    - Display caller ID info
    - Identify themselves and what they are selling
    - Disclose all material info and terms
    - Comply with special rules for prizes and promotions
    - Respect requests to call back
    - Retain records for at least 24 hours
    - Comply with special rules for automated dialers

- Required disclosures before delivering sales content:
    - Identity of seller
    - Purpose of the call is to sell goods/services
    - Nature of goods/services
    - No purchase or payment is necessary to participate to win prize/promotion and does not increase chances of winning
- Ten broad categories of info that must always be disclosed:
    - Cost and quantity
    - Material restrictions, limitations, conditions
    - Performance, efficacy, central characteristics
    - Refund, repurchase, or cancellation policies
    - Material aspects of prize promotions
    - Material aspect of investment opportunities
    - Affiliations, endorsements, or sponsorships
    - Credit card loss protection
    - Negative option features
    - Debt relief services
- Call Abandonment expressly prohibited: telemarketer does not connect the call to a live sales rep within two seconds of the person's completed greeting. Pre-recorded sales pitches are not allowed (must have opt in from consumer)
    - Abandonment Safe Harbor:
        - Use tech that ensure abandonment of no more than three percent of all calls answered by live person measured per day per calling campaign
        - Allows telephone to ring for 15 seconds or four rings before disconnecting unanswered call
        - Plays recorded message stating name and phone number of seller on whose behalf the call was placed whenever a live sales rep is unavailable w/in 2 secs of a live person answering
        - Maintains records documenting adherence to the preceding three reqs
- Requires sellers and telemarketers to keep substantial records:
    - Advertising and promotional materials
    - Information about prize recipients
    - Sales records
    - Employee records
    - All verifiable authorizations or records of express informed consent or express agreement
- For each record above, sales records must include:
    - The name and last known home address of each customer
    - Goods or services to be purchased
    - The date the goods or services were shipped/provided
    - The amount the customer paid for goods/services
- For all former and current employees involved in sales above:
    - Their name
    - The last known home address and phone number

    - Job titles
- Other provisions to address:
    - Credit card laundering
    - Telemarketing sales of credit repair programs, loss recovery services and advance loans
    - Telefunding activities (for-profit companies that call on behalf of charitable orgs)
- **Updates to the Telephone Consumer Protection Act (TCPA)**
    - Even if a company has an EBR, it is required to receive prior express written consent for all robocalls to residential lines.
    - Consumers allowed to opt out of future robocalls during a robocall
    - Robocalls to residential lines made by healthcare related entities governed by HIPAA are exempt from these requirements (Ex: CVS pharmacy robocall)
    - Robotexts require express consent
        - Consent can be revoked at any time by any reasonable means
        - The mere fact that a consumer's wireless number appears in the contact list of another wireless customer is not sufficient to establish consent
        - When a caller has consent for a wireless number and the number has been reassigned, the caller is not liable for the first call but will be liable for subsequent calls if the new consumer makes the caller aware of the change

The Telephone Consumer Protection Act of 1991 (TCPA)

- Enforced by the FCC
- Prohibits unsolicited commercial fax transmissions
    - Penalties: private right of action and statutory damages of up to $500/fax
- Preempts interstate regulation
- Does not preempt within states (CA attempted to eliminate the EBR requirement)

The Junk Fax Prevention Act of 2005 (JFPA)

- Consent required for commercial faxing
- Consent can be inferred from an EBR and it permits sending of commercial faxes to recipients based on EBR as long as the sender offers an opt out in accordance with the act
- EBR has same definition as FTC's DNC rule

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)

- No private right to action
- Preempts most state spam laws
    - State spam laws are not superseded to the extent that such laws prohibit false or deceptive activity
- **Enforcement:** FTC, other federal regulators, state AGs and other state officials
- **Violation:** fines up to $40,654/violation. For those authorized to sue (ISP's can sue violators), the act provides for injunctive relief and damages up to $250/violation with a max of $2 mil. A court may increase a damage aware up to three times the amount in cases of willful or aggravated violations

- Covers transmission of commercial email messages whose primary purpose is advertising or promoting a product or service
    - Prohibits false or misleading headers
    - Prohibits deceptive subject lines
    - Requires commercial emails to contain a functioning, clearly and conspicuously displayed return email address that allows the recipient to contact the sender
    - Requires clear and conspicuous notice of the opportunity to opt out such as by return email or an opt out link
    - Prohibits sending commercial email (following a grace period of 10 business days) to an individual who has asked to not receive future email
    - Requires all commercial email to include:
        - Clear and conspicuous identification that the message is a commercial message (unless affirmative consent was provided) and
        - A valid physical address of the sender
    - Prohibits aggravated violations relating to commercial email such as
        - Address-harvesting and dictionary attacks
        - Automated creation of multiple email accounts
        - Retransmission of commercial email through unauthorized accounts
    - Requires all email containing sexually oriented material to include a warning label (unless the recipient has provided prior affirmative consent to receive the email)
- Rules cover messages sent using SMS but do not cover phone to phone messages
- Prohibits senders from sending MSCMs without the subscriber's express prior authorization
    - Must be opt in (check box on a website can't be pre-checked)
    - Authorization must be given prior to the sending of any MSCMs
    - Consumers must not bear any costs with authorization/revocation
    - Each authorization must include certain required disclosure stating:
        - The subscriber is agreeing to receive MSCMs sent to his or her wireless device from a particular (identified) sender
        - The subscriber may be charged by his or her wireless provider in connection with the receipt of such messages
        - The subscriber may revoke the authorization at any time
    - Disclosures must be clear and conspicuous
    - Authorization must be specific to the sender and must clearly identify the entity (no third parties)
    - Authorization must be obtained in any format and must be documented
    - Senders must enable consumers to revoke authorizations by the same means of revocation
    - MSCMs themselves must include functioning return email addresses or another Internet based mechanism that is clearly and conspicuously displayed for the purpose of receiving opt outs
    - 10 business day grace period following revoked authorization

The Telecommunications Act of 1996

- Section 222 governs the privacy of customer info provided to and obtained by telecommunications carriers. Prior, carriers were permitted to sell consumer data to third parties w/o consent. This statute imposes new restrictions on the access, use, and disclosure of customer proprietary network info (CPNI)
- ISPs are subject to general CPNI requirements
- Carriers can use and disclose CPNI only with customer approval or as required by law
- FCC governs
- U.S West Inc v FCC made standard switch to opt out for carrier's own use of CPNI
- Carriers must obtain express consent to share data with third parties. Sharing is allowed with joint venture or independent contractors unless customers opted out within 30 days of being notified. Must opt in if the data shared will be for marketing purposes
- Other requirements:
    - Carriers must notify law enforcement when CPNI is disclosed in a security breach w/in seven business days of the breach
    - Customers must provide a password before they can access their CPNI via telephone or online account services
    - Carriers must certify their compliance with these laws annually, explain how their systems ensure compliance and provide an annual summary of consumer complaints related to unauthorized disclosure of CPNI

The Cable Communications Policy Act of 1984

- Provides private right of action
- Excludes internet services via cable
- Defines cable service" one way transmission to subscribers of video programming or other programming service and subscriber interaction if any which is required for the selection of such video programming or other programming service
- Cable service providers must give a privacy notice that clearly and conspicuously informs subscribers of
    - The nature of the PI collected
    - How such info will be used
    - The retention period of such info
    - The manner by which the subscriber can access and correct such info
- A Cable provider can only collect PI that is necessary to render cable services or detect the unauthorized reception of services
- Limits cable service providers right to disseminate PI without written or electronic consent. Exceptions:
    - To the extent necessary to render services or conduct other legit business activities
    - Subject to a court order with notice to the subscriber
    - If the disclosure is limited to the name and addresses and the subscriber is given an option to opt out
- Mandates PI be destroyed when it is no longer needed for the purpose for which it was collected and there are no pending requests for access

- Conflicts with the ECPA's provision that no notice is needed for court orders. Courts rule in favor of ECPA

The Video Privacy Protection Act of 1988 (VPPA)

- Private right of action for violations. Statutory damages set at $2,500. Also allows for actual, punitive, and reasonable attorney fees.
- Not applicable to video streaming
- Does not preempt more protective state laws
    - California has enacted laws covering the same privacy issues as VPPA
- Applies to video tape service providers who are defined as anyone engaged in the business in or affecting interstate or foreign commerce, of rental, sale or delivery of pre-recorded video cassette tapes or similar audio-visual materials as well as individuals who receive PI in the ordinary course of a videotape service provider's business or for marketing purposes
- Videotape service providers are prohibited from disclosing PI. Exceptions:
    - Disclosure is made to the consumer themselves
    - Is made subject to the contemporaneous written consent of the consumer
    - Is made to law enforcement pursuant to a warrant, subpoena or other court order
    - Includes only the names and addresses of consumers
    - Includes only names, addresses and subject matter descriptions and the disclosure is only use for the marketing of goods or services to the consumers
    - Is for order fulfillment, request processing, transfer of ownership or debt collection
    - Is pursuant to a court order in a civil proceeding and the consumer is granted a right to object
- PI must be destroyed as soon as practicable but no later than one year from the date the info is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such info
- **The Video Privacy Protection Act Amendments Act of 2012**
    - Allowed for one-time consumer consent that was valid for up to two years replacing the contemporaneity requirement
    - Addresses social media concerns

The California Online Privacy Protection Act of 2013 (CalOPPA)

- Amended by Assembly Bill 370
    - Required privacy policies to include information on how the operator responds to Do Not Track signals or similar mechanisms.
    - Requires privacy policies to state whether third parties can collect PII about the site's users
    - Requires the operator of a website to display a privacy notice that meets certain content requirements. These include disclosing:
        - Categories of PII collected through the site
        - Categories of third party entities with whom the operator may share PII or other content
        - How the operator responds to the web browser's Do Not Track signals or other mechanisms that provide consumers the ability to choose regarding collection

of PII about an individual consumer's online activities over time and across third party websites
    - Whether other parties may collect PII about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website.

Online Privacy

Children's Online Privacy Protection Act (COPPA)

- Passed specifically to protect children's use of the Internet, particularly websites and services targeted toward children.
- Does not preempt state laws
    - **California's Privacy Rights for California Minors in the Digital World**
        - Individuals under age of 18 have the right to request removal of info posted online
        - Prohibits online advertising to minors related to products that these consumers are not legally permitted to buy and also restricts certain online advertising practices based on the minors' P.I
    - **Delaware's Online and Personal Privacy Protection Act**
        - Contains similar categories of restrictions related to advertising to minors
- No private right of action
- Requires website operators to provide clear and conspicuous notice of the data collection methods employed by the website, including functioning hyperlinks to the website privacy policy on every web page where personal info is collected.
- Requires consent by parents prior to collection of personal info for children under 13
- No mention of a national security exception for disclosure

The EU Data Protection Directive

- Implements what the EU considers the data subject's fundamental right to access and correct personal info about the data subject
- **The Privacy Shield**
    - Example of a lawful basis for transferring personal data from the EU to the U.S
    - Includes specific provisions about access and correction as does the Asia-Pacific Economic Cooperation (APEC) Privacy Framework
- **The EU Cookie Directive**
    - Requires that users give consent before having cookies placed on their computers, thereby preventing cookie tracking of their online activities if they do not opt in
    - The EU Electronic Privacy Directive of 2002 has taken the position that info stored in cookies is generally personal data (so users must consent)

Web Cookies best practices:

- Not store unencrypted personal info

- Provide adequate notice of their usage
- Use a persistent variation only if the need justifies it
- Not set long expiration dates
- Disclose the involvement of a third-party cookie provider (if applicable) as well as an opt out (or in Europe, an opt in) mechanism for delivery from that third party

Workplace Privacy

Note: Employee privacy is protected by several federal agencies including the U.S Department of Labor (DOL), the Equal Employment Opportunity Commission (EEOC), the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and the National Labor Relations Board (NLRB)

The Consolidated Omnibus Budget Reconciliation Act (COBRA)

- Requires qualified health plans to provide continuous coverage after termination to certain beneficiaries

The Employee Retirement Income Security Act (ERISA)

- Ensures that employee benefit programs are created fairly and administered properly

The Family and Medical Leave Act (FMLA)

- Entitles certain employees to unpaid leave in the event of birth or illness of self or a family member

The Fair Labors Standards Act (FLSA)

- Establishes minimum wage and sets standards for fair pay

The Occupational Safety and Health Act (OSHA)

- Regulates workplace safety

The Whistleblower Protection Act

- Protects federal employees and applicants for employment who claim to have been subjected to personnel actions because of whistleblowing activities

The National Labor Relations Act (NLRA)

- Sets standards for collective bargaining, which also applies in social media communications

The Immigration Reform and Control Act (ICRA)

- Requires employment eligibility verification

The Americans with Disabilities Act (ADA)

- Forbids employers with 15 or more employees from discriminating against a qualified individual with a disability because of the disability of such individual
- Before an offer of an employment is made, the ADA permits such examinations and medical inquiries only where job related and consistent with business necessity
- A company may require a medical examination after the offer of employment has been made and may condition the offer on the results of such an exam. The exam is permitted if:
    - All entering employees are subjected to the exam
    - Confidentiality rules are followed for the results of the exam
    - The results are only in accordance with the statutory prohibitions against discrimination on the basis of disability
- Employer must provide reasonable accommodations during employment but employers are not permitted to ask about accommodations before a conditional offer is made
- The ADA Amendments Act (ADAAA) significantly expanded the scope of conditions that are mitigated, in remission or episodic if they would substantially limit a major life activity of an employee when active or absent mitigation.

The Employee Polygraph Protection Act of 1988 (EPPA)

- Limits employer use of lie detectors
- Private right of action
- Does not preempt stricter state laws
- Issued by DOL, employers are prohibited from using lie detectors on incumbent workers or to screen applicants
    - Exceptions for government employees, those engaged in the manufacture of controlled substances, certain defense contractors, and those in certain national security functions
    - Also allowed in connection with an ongoing investigation involving economic loss or injury to the employer's business. Must be reasonable suspicion to test.
- Employers must post the act's essential provisions in a conspicuous location so that employees are aware of its existence
- **Violations:** subject to fine by DOL and private lawsuits

Anti-Discrimination laws:

- Title VII of the Civil Rights Act of 1964 bars discrimination in employment due to race, color, religion, sex, and national origin
- The Equal Pay Act of 1963 bars wage disparity based on sex
- The Age Discrimination Act bars discrimination against individuals over 40
- The Pregnancy Discrimination Act bars discrimination due to pregnancy, childbirth, and related medical conditions
- The Americans with Disabilities Act of 1990 bars discrimination against qualified individuals with disabilities
- The Genetic Information Nondiscrimination Act of 2008 bars discrimination based on individuals' genetic info

- The Bankruptcy Act provision 11 U.S.C 525 (b) prohibits employment discrimination against persons who have filed for bankruptcy

The California Investigative Consumer Reporting Agencies Act (ICRAA)

- Employers must notify applicants and employees of their intention to obtain and use a consumer report.
- Employer must obtain the applicant or employee's written authorization prior to requesting the report
- If employers wish to take adverse action based on the report, they must provide employees with a copy of the report regardless of whether the employee waived the right to receive a copy. This exception does not apply to employees suspected of wrongdoing or misconduct.
- Must obtain consent every time a background check is initiated
- The written disclosure must state:
    - The fact that a report may be obtained
    - The permissible purpose of the report
    - The fact that the disclosure may include info on the consumer's character, general reputation, personal characteristics, and mode of living
    - The name, address, and phone number of the investigative consumer reporting agency
    - As of 2012, it must also include the CRA's website
- Note, under FCRA, the employer doesn't need consent if they're performing the background check themselves. ICRAA requires that employer gives a copy of internal records to the employee or applicant unless they waive the right

Federal Drug Testing Law

- Mandated for:
    - Positions within the federal sector
    - Employees of the U.S CBP
    - Aviation
    - Railroading
    - Trucking industries
- Rules preempt state laws that would otherwise limit drug testing
- Types:
    - Preemployment: generally allowed if not designed to identify legal use or addiction
    - Reasonable suspicion: generally allowed as a condition to continued employment based on specific facts of evidence and inferences from those facts
    - Routine testing: generally allowed if employees are notified at the time of hire
    - Post-accident testing: generally allowed as continued employment if reasonable suspicion accident took place due to substance use
    - Random testing: sometimes required by law, prohibited in certain jurisdictions, acceptable where used on existing employees in specific narrowly defined jobs such as those in highly regulated industries where the employee has severely diminished expectation of privacy or where testing is critical to public safety or national security

Civil Litigation and Government Investigation Privacy

The Electronic Communications Privacy Act (ECPA)

- Private right of action and criminal penalties
- Does not generally preempt stricter state privacy protections
    - Some state laws protect email communications
- Generally strict in prohibiting interception of wire communications such as telephone calls or sound recordings from video cameras; oral communications such as hidden bugs or microphones; and electronic communication such as emails
- Unless exception applies, interception of these communications is a criminal offense
- Two exceptions for workplace monitoring:
    - If a person is a party to a call or where one of the parties has given consent
    - The interception is done in the ordinary course of business
    - Note: some states require all party consent to listen versus one party consent
- Provided for a pen register and trap and trace orders from a judge under the standard of "relevant to an ongoing investigation."

The Stored Communications Act (SCA)

- Private right of action and criminal penalties
- Part of the ECPA
- Creates a general prohibition against the unauthorized acquisition, alteration, or blocking of electronic communications while in electronic storage in a facility through which an electronic communications service is provided.
- Two exceptions for employers:
    - By the person or entity providing the wire or electronic communication service
    - By a user of that service with respect to a communication of or intended for that user
- A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall tall all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process
- In Microsoft v U.S case, SCA did not require the company to provide electronic evidence that was stored outside the U.S

The USA Patriot Act

- Section 217 permits, but does not require, the owner or operator of a computer system to provide such access in defined circumstances. For computer trespassers, law enforcement can now perform interceptions if:
    - The owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer
    - The person acting under color of law is lawfully engaged in an investigation

    - The person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation
    - Such interception does not require communications other than those transmitted
- Expanded definition of pen register/trap and trace beyond telephone numbers to include dialing, routing, addressing, or signaling info
- Section 215: provides that a federal court order can require the production of any tangible thing for defined foreign intelligence and anti-terrorism investigations
    - Disclosure is permitted to the persons necessary to comply with the order and to an attorney
- Expanded the use of National Security Letters
    - Included strict rules against disclosing that an org had received an NSL
    - 2006 amendment said that recipients are bound to the confidentiality only if there is a finding by the requesting agency of interference with criminal or counterterrorism investigation or for other listed purposes
    - Recipients could petition the court to modify or end the secrecy requirement
    - As of 2015, the FBI now presumptively terminates NSL secrecy for an individual order when an investigation closes, or no more than three years after the opening of a full investigation

USA FREEDOM Act

- Set new rules for national security investigations prohibiting the use of pen register/trap and trace orders for bulk collection and restricting their use to circumstances where there were specific selectors such as an email address or telephone number.
- Ended bulk collection of Section 215 PATRIOT ACT

The Judicial Redress Act of 2016

- Extends U.S Privacy Act protections to certain non-U.S persons

The Communications Assistance to Law Enforcement Act (CALEA)

- Aka Digital Telephony Bill
- Lays out the duties of defined actors in the telecommunications industry to cooperate in the interception of communications for law enforcement and other needs relating to the security and safety of the public.
- Requires telecommunications carriers to design their products and services to ensure that they can carry out a lawful order to provide gov access to communications.
- FCC implemented CALEA
- Applies to telecommunications carriers but not other information services
    - VOIP is considered a telecommunication service and must operate under CALEA requirements

The Cybersecurity Information Sharing Act (CISA) 2015

- Permits the federal gov to share unclassified technical data with companies about how networks have been attacked and how successful defenses against such attacks have been carried out. CISA encourages companies to voluntarily share the same info with gov
- Company's release of info about cyber threat indicators and defensive measures receive certain protections
    - Limitations on liability
    - Non-waiver of privileges
    - Exemption from FOIA disclosure
- Provisions:
    - Authorization for a company to share or receive cyber threat indicators or defensive measures
    - Requirement for company to remove personal info before sharing
    - Sharing info with federal gov does not waive privileges (no similar provision for sharing with state/local gov)
    - Share info exempt from federal and state FOIA laws
    - Prohibition on gov using shared info to regulate or take enforcement actions against lawful activities
    - Authorization for company's monitoring and operating defensive measures
    - Protection from liability for monitoring activities

Right to Financial Privacy Act (RFPA)

- Apply to disclosures by a variety of financial institutions including banks, credit card companies, and consumer finance companies
- No gov authority may have access to or obtain copies of or information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and meet one of these conditions:
    - The customer authorizes access
    - There is an appropriate admin subpoena or summons
    - There is a qualified search warrant
    - There is an appropriate judicial subpoena
    - There is an appropriate formal written request from an authorized gov authority
- Only applies to requests from federal agencies
- Customers must receive notice in advance of the gov request for the records and they have a right to challenge disclosure

The Privacy Protection Act (PPA)

- Does not preempt state laws
- Provides an extra layer of protection for members of the media and media orgs from gov search or seizures in the course of criminal investigation
- Effectively forces law enforcement to use subpoenas or voluntary cooperation to obtain evidence from those engaged in First Amendment activities
- Applies to gov officers or employees at all levels of gov
- Applies to criminal investigations (not civil)

- **Violations:** $1,000 actual damages and attorney's fees
- Exception: Probably cause that reporter is involved or in the process of committing a crime

The Federal Freedom of Information Act (FOIA)

- Public access to gov records

The Foreign Intelligence Surveillance Act (FISA)

- Establishes standards and procedures for electronic surveillance that collects foreign intelligence within the U.S. FISA orders can issue when foreign intelligence gathering is a significant purpose of the investigation.
- Orders issue from a special court of federal district court judges, the Foreign Intelligence Surveillance Court (FISC).
- FISA authorizes wiretap orders, pen register, and trap and trace orders (for phone numbers, email addresses, and other addressing and routing info) and orders for video surveillance
- Entities that receive FISA orders to produce records generally cannot disclose the fact of the order to targets of the investigation. There is generally no disclosure after the fact to the target of a FISA wiretap as there is for law enforcement wiretaps.
- **Section 702** refers to a provision in the FISA Amendments Act which revised FISA
    - Applies to a collection of electronic communications of targeted individuals for listed foreign intelligence purposes
    - Must annually approve certifications by the director of national intelligence and the attorney general setting the terms for section 702 surveillance. To target the communications of any person, the gov must have a foreign intelligence purpose to conduct the collection and a reasonable belief that the person is a non-U.S citizen located outside the U.S
    - Two surveillance programs:
        - **PRISM:** collection, acting under a section 702 court order, the government sends a judicially approved and judicially supervised directive requiring collection of certain selectors such as an email address. The company's lawyers have the opportunity to challenge the request
        - **Upstream:** targets Internet based communications as they pass through physical Internet infrastructure located w/in the U.S. Designed to only acquire Internet communications that contain a tasked selector. Emails and other transactions that make it through the filters are stored for access by the NSA, while info that does not make it through the filters is never accessed by the NSA or anyone else.