**U.S. Private-Sector Privacy Certification**

**Outline of the Fall 2020 BoK for the CIPP/US**

1. **INTRODUCTION TO THE U.S. PRIVACY ENVIRONMENT (28-34 QUESTIONS)**
	1. **STRUCTURE OF U.S. LAW** **(6-9 QUESTIONS)**
		1. **Branches of government**

Designed to provide both a separation of powers and a system of checks and balances. When authorized by Congress, federal agencies promulgate and enforce rules pursuant to the law

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Legislative** | **Executive** | **Judicial** |
| **Purpose** | Makes laws | Enforces laws | Interprets laws |
| **Who** | Congress (House & Senate) | Pres., VP, Cabinet, Federal Agencies (e.g., FTC) | Federal Courts |
| **Checks & Balances** | Congress confirms presidential appointee, can override vetoes | President appoints federal judges, can veto laws passed by Congress | Determines whether laws are constitutional |

* + 1. **Sources of law**
			1. **Constitutions**: US Const. does not contain the word privacy, but some parts directly affect privacy (e.g., 4th amendment limits on govt searches). State constitutions can create stronger rights than US Const. (e.g., CA state constitution expressly recognizes right to privacy)
			2. **Legislation**: State legislation may be stricter than national legislation. Federal law overrides state laws, as with HIPAA and CAN-SPAM (field preemption or conf and rules that place compliance expectations on industries, such as marketing
			3. **Case law**: Judges’ final decisions. Precedents change as technological and societal changes in values and laws evolve over time
			4. **Common law**: Legal principles that have developed over time through judicial decisions (case law) in contrast with statutory laws. Doctor-patient and attorney-client privilege / confidentiality are CL
			5. **Contract law**: Legally binding K (offer, acceptance, consideration, legal purpose). K may be unenforceable, e.g., due to a conflict with public policy or misrepresentation/fraud. Privacy notice may be a contract if consumer provides data to company based on company’s promise to use data as stated in notice
		2. **Legal definitions**
			1. **Jurisdiction**: the authority of a court to hear a particular case. Need both subject matter jurisdiction (type of dispute) and personal jurisdiction (the parties to the dispute)
			2. **Person**: any entity with legal rights, including an individual (a “natural person”) or a corporation (a “legal person”)
			3. **Preemption**: a superior government’s ability to have its laws supersede those of an inferior government (e.g., Fed mandate that states can’t regulate email marketing – CAN-SPAM preempts state laws that might impose greater obligations on senders of commercial e-mail)
			4. **Private right of action**: the ability of an individual harmed by a violation of a law to file a lawsuit against the violator
			5. **Notice**: a description of an organization’s information management practices (what information is collected, how the information is used and disclosed, how to exercise any choices about uses or disclosures, and whether the individual can access or update the information). 2 **purposes**: **consumer education** and **corporate accountability**
			6. **Choice**: the ability to specify whether personal information will be collected and/or how it will be used or disclosed. Can be express or implied but must be meaningful (i.e., based on a real understanding of the implications of the decision)
				1. **Opt-in** – affirmative indication of choice based on an express act of the person giving consent
				2. **Opt-out** – choice is implied by failure of the person to object to the use or disclosure
			7. **Access**: the ability to view personal information held by an organization; may be supplemented by allowing updates or corrections to the information
		3. **Regulatory authorities**

U.S. has no national data protection authority, but several groups oversee privacy matters

* + - 1. **Federal Trade Commission (FTC)**: independent agency governed by chairperson +4 other commissioners whose decisions are NOT under President’s direct control. Founded in 1914 to enforce antitrust laws. Consumer protection mission established by a statutory change in 1938. Privacy and computer security are now large part of its role. **General authority** to enforce rules against “unfair and deceptive trade practices.” This includes the power to bring deception enforcement actions (under Section 5 of the FTC Act) where an organization has broken a privacy promise. Also has specific statutory responsibility (i.e., **specific authority**) for issues such as children’s online privacy and commercial email marketing and has been instrumental in developing U.S. privacy standards. In recent years, more prominent role in enforcement.
				1. **Section 6** vests the commission with the authority to conduct investigations and to require businesses to submit investigatory reports under oath
				2. **Section 5** applies to unfair or deceptive acts or practices in or affecting commerce but does not apply to nonprofit organizations. Described as **perhaps single most important piece of US privacy law**. Applies to privacy and info sec. Does not apply to banks, other federally regulated financial institutions or common carriers (e.g., transportation and communications industries)
				3. FTC is **rule-making and enforcement agency** for **COPPA**, **CAN-SPAM**, Telemarketing Sales Rule (**TSR**) (shared with FCC), **HITECH** (along with HHS)
				4. **Sunset policy** - administrative orders such as consent decrees are imposed for up to 20 years
				5. **HIPAA, Gramm-Leach-Bliley, and COPPA impose notice requirements**. CA requires companies and organizations doing in-state business to post privacy policies on their website
			2. **Federal Communications Commission (FCC)**: places significant compliance regulations on the marketplace. Governs communications industry (TV, radio, online). Enforces privacy laws along with the FTC anytime TSR (telemarketing) involved
			3. **Department of Commerce (DoC)**: plays a leading role in federal privacy policy development and administered the privacy shield framework between the US and the EU. Works along with the FTC on the enforcement of privacy and security standards set by organizations, particularly with those having privacy self-regulatory programs
			4. **Department of Health and Human Services (HHS)**: created regulations to protect the privacy and security of healthcare information. Responsible for enforcement of HIPAA laws. Shares rule-making and enforcement power with the FTC for data breaches related to medical records under the HITECH act
			5. **Department of Justice (DoJ)**: sole federal agency to bring criminal enforcement actions, which can result in imprisonment or criminal fines. HIPAA provides for both civil and criminal enforcement, and procedures exist for roles of both HHS and DOJ
			6. **US office of management and budget (OMB)**: lead agency for interpreting privacy act of 1974, which applies to federal agencies and private-sector contractors to those agencies. Also issues guidelines to agencies and contractors on privacy and information security issues.
			7. **Banking regulators**
				1. **Federal Reserve Board**: enforces provisions by specific financial mandates, like GLBA. The consumer financial protection bureau is an independent bureau under the federal reserve, has rule-making authority for laws related to financial privacy and oversees the relationship between consumers and financial product and service providers
				2. **Office of Comptroller of the Currency (OCC)**: independent bureau of the U.S. department of the treasury. Regulates and supervises all national and federal banks and savings institutions, including agencies of foreign banks, OCC ensures fair access to financial services and compliance with financial privacy laws and regulations
			8. **State attorneys general**: the chief legal advisor to the state government as well as the state’s chief law enforcement officer. They may take enforcement action on a state’s unfair and deceptive practice laws, HIPAA, GLBA, the telemarketing sales rule and violations of breach notification laws
			9. **Self-regulatory programs and trust marks**: self-regulatory models emphasize creation of codes of practice for protection of PI by a company, industry or independent body. Many industry groups create and monitor their own privacy guidelines and practices. Government agencies, such as the FTC, may be involved in enforcement and adjudication. Organizations may also adopt guidelines of a 3rd party and have that 3rd party monitor and enforce compliance (3rd party seal and certification programs: TrustArc, Better Business Bureau, and the EU-US privacy shield)
				1. **Payment Card Industry Data Security Standard (PCI DSS)**: an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. Maintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.
		1. **Understanding laws**

Privacy compliance requires knowing the applicable legal rules as well as fulfilling each organization’s policies and goals.

* + - 1. **Scope and Application**: who is covered by the law, what types of info are covered
			2. **Analyzing a law**
				1. **How to Comply**: what exactly is required/prohibited
				2. **Assess Risk**: who enforces the law, consequences of noncompliance
				3. **Motivation for the Law**: why does the law exist
			3. **Determining jurisdiction**:
			4. **Preemption**:
	1. **ENFORCEMENT OF U.S. PRIVACY AND SECURITY LAWS (3-5 QUESTIONS)**

3 categories of legal action: **civil litigation, criminal prosecution, administrative enforcement**

* + 1. **Criminal versus civil liability**
			1. **Criminal prosecution**: lawsuit brought by govt for violation of criminal laws; can lead to imprisonment and criminal fines. DoJ prosecutes violations of federal criminal law. Violations of state criminal law handled by state attorney general and local officials (district attorneys)
			2. **Civil litigation**: effort by private party to correct specific harms - negligence, breach of warranty, misrepresentation, defamation, strict tort liability, or statutory actions. Some privacy laws create private right of action enabling individual to sue based on violations of the statute.
			3. **Administrative Enforcement**: carried out pursuant to statutes that create and empower the agency, such as the FTC or FCC, under the Administrative Procedures Act (APA) with hearings before administrative law judge (ALJ). Agency adjudications can be appealed to federal court. Agency can sue a party in federal court with agency as plaintiff in civil action. Administrative enforcement through consent decree is a judgment entered by consent of the federal or state agency and the adverse party. In the form of a legal document that has been approved by a judge, it specifies action, such as ceasing alleged illegal activity, and can carry fines.
		2. **General theories of legal liability**
			1. Contract
			2. **Tort**: civil wrongs that result in injury or harm and are recognized by law as the grounds for lawsuits. Goals are to provide relief for damages incurred and deter others from doing the same thing (intentional (knew or should have known), negligence (unreasonable), and strict liability (no need for negligence or intent)
				1. **Strict Liability**: standard commonly used for **civil violations**
				2. **Intentional Tort: Invasion of Privacy**

 **Intrusion upon solitude**

Defendant intentionally invaded plaintiff's privacy - intruded into private affairs or seclusion.

Intrusion would be objectionable or highly offensive to a reasonable person.

Intrusion was on a private matter of plaintiff.

Intrusion caused plaintiff emotional anguish or suffering.

**Appropriation of Name or Likeness**

Defendant utilized some protected aspect of plaintiff’s identity

Without consent

For immediate and direct benefit

**False Light**

Defendant publicly disclosed potentially misleading or damaging information about plaintiff (even if true);

Information placed plaintiff in false light

The false light would be highly offensive to reasonable person

**Public Disclosure of Private Facts**

Defendant publicized a matter regarding private life of plaintiff

Publicized matter would be highly offensive to reasonable person

Not of legitimate concern to the public

* + - 1. Civil enforcement: administrative
		1. **Negligence**: defendant’s actions were unreasonably unsafe; for example, causing a car accident by not obeying traffic rules or not having appropriate security controls
		2. **Unfair or deceptive trade practices (UDTP)**: FTC has enforcement authority over an organization’s deceptive and unfair trade practices.
			1. **Deceptive practices** may include false promises, misrepresentations and failure to comply with representations made to consumers. **Privacy practices** cases. **Elements**:
				1. Must involve a **misleading act** (representation, omission or practice) of the business
				2. Must be analyzed from the perspective of a **reasonable consumer**
				3. Must be **material** – likely to affect consumer’s behavior
			2. **Unfair practices** may include failure to implement adequate protection measures for sensitive personal information or providing inadequate disclosures to consumers. **Security breach** cases. **Elements**:
				1. Must cause or be likely to cause **substantial injury** to consumer
				2. Must **not be reasonably avoidable** by consumer
				3. Must **not be outweighed by the benefits** to consumer
		3. **Federal enforcement actions**: **FTC** cannot assess fines, but can recommend fines (up to 16K). Read press/or someone complains, FTC conducts investigation, then may try to reach an agreement before going to court. Following an investigation, FTC may initiate an enforcement action if it has reason to believe a law is being or has been violated. The commission issues a complaint, and an administrative trial can proceed before an ALJ, if a violation is found, ALJ can enjoin the company from continuing the practices that caused the violation. ALJ decision can be appealed to the five commissioners, which can in turn be appealed to federal district court. An order by the commission becomes final 60 days after it is served on the company. If an FTC ruling is ignored the FTC can seek civil penalties in fed court up to $40K/violation
			1. **Geocities (suspected deceptive practice)**: sold user info to 3rd parties, violating their own privacy notice on their websites. Settled, FTC issued consent order requiring Geocities to post and adhere to a **conspicuous online privacy notice** that disclosed to users how it would collect and use personal information
			2. **Eli Lilly**:users could provide personal information for messages and updates reminding them to take their medication. Eli Lilly emailed subscribers they were ending the program, inadvertently addressed to and revealing the email addresses of all subscribers. FTC **required** Eli Lilly **to develop and maintain** an **information privacy and security program for the first time**. This case expanded the scope of settlement terms to include implementation and evaluation of company programs for processing personal information.
			3. **Snapchat (suspected deceptive practices)**: Knew there were many ways to save a snapchat and were collecting names/phone numbers of all contacts in user’s address book, which could be hacked. Consent order with FTC agreeing hey would not engage in these practices for next 20 years
			4. **Lifelock (suspected unfair practice)**: **failed to encrypt customers data or properly restrict access** to data held by the company. Consent order to pay significant fines and then had to pay out millions for failure to comply with the 2010 consent order.
			5. **Wyndham Worldwide Corp (suspected unfair practice)**: **failed to implement standard security controls**. Did not adequately protect its sensitive data. Entered consent order with the FTC. Extended FTC’s longstanding authority to regulate unfair methods of competition in or affecting commerce to regulation of cyberspace practices that are harmful to consumers
			6. **Consent decree**: party does not admit fault, but promises to change its practices and avoids further litigation on the issue. Can seek **fines in fed court if a consent decree violated**. Under FTC’s “**sunset policy**” administrative orders such as consent decrees are imposed for **up to 20 years**. Added requirement of a comprehensive privacy program in 2009.
			7. “**Deceptive**”: for a practice to be deceptive, it must involve a material statement or omission that is likely to mislead consumer who is acting reasonably under the circumstances. Deceptive practices include false promises, misrepresentations, and failures to comply with representations made to consumers.
			8. “**Unfair**”: FTC has sanctioned companies for unfair practices when there’s a failure to implement adequate protection measures for sensitive personal info or when they provided inadequate disclosures to consumers
		4. **State enforcement (Attorneys General (AGs), etc.)**: each state has laws similar to the FTC Act section 5 (unfair or deceptive acts and practices, UDAP) which are enforced by state attorneys general. Some states also allow enforcement against unconscionable practices
		5. **Cross-border enforcement issues (Global Privacy Enforcement Network (GPEN))**: when organizations and government agencies are in more than one jurisdiction, cooperation must exist between enforcement agencies
			1. **Cooperation between enforcement agencies**: engaging in closer cooperation - 2007 OECD Recommendation on cross-border co-operation: discuss the practical aspects of privacy law enforcement cooperation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness campaigns. Led to establishment of global privacy enforcement network (GPEN) in 2010 by FTC and enforcement authorities. **GPEN aims to promote cross border information sharing as well as investigation and enforcement cooperation among privacy authorities around the world**. The APEC Cross-Border Privacy Enforcement Arrangement (CPEA) aims to establish a framework for participating members to share information and evidence in cross-border investigations and enforcement actions in the Asia-Pacific region. FTC is a CPEA participant and provides updates in its yearly privacy & security report.
			2. **Conflicts between Privacy and Disclosure Laws**: conflicts can arise when the privacy laws in one country prohibit disclosure of information but laws in a different country compel disclosure.
		6. **Self-regulatory enforcement (PCI DSS, Trust Marks)**: self-regulatory approaches to privacy protection have been created by some organizations, through which they monitor their own privacy guidelines and practices. Organizations may also adopt the guidelines of a third party that monitors and enforces compliance. Self-regulation only occurs at the quasi-legislation stage. A company writes its own privacy policy, or an industry group drafts a code of conduct that companies agree to follow. Adjudication refers to the question of who should decide whether a company has violated the privacy rules and with which penalties – takes place before ALJ with appeal to federal court (FTC can still be involved at enforcement and adjudication stage).
		7. **2012 Federal Privacy Reports**: 2012 Obama issued “consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy,” which is the White House report. FTC issued “Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers,” which is the FTC report. **These two reports together indicate a significantly more comprehensive approach to privacy protection and enforcement**.
			1. FTC late 1990s was **“notice and choice”** approach. 2001-2009 emphasized **harm based model**. In 2009 began to implement requirement of a comprehensive privacy program in **consent decrees** (which is **reflected in** the **2012 White House AND FTC reports**).
			2. **2012 White House report** emphasizes
				1. **Individual control** over what personal data collected and how it’s used
				2. **Transparency**: privacy and security practices should be easily understandable and accessible
				3. **Respect for context**: consumer right to expect that personal data will be collected, used and disclosed consistent with context in which the personal data was provided
				4. **Security**: consumer right to secure and responsible handling of personal data
				5. **Access and accuracy**: consumer right to access and correct personal data in usable format, appropriate to the sensitivity of the data and the risk of adverse consequences if data inaccurate
				6. **Focused collection**: consumer right to reasonable limits on personal data collected and retained
				7. **Accountability**: consumer right to have personal data handled with appropriate measures in place to ensure adherence to Consumer Privacy Bill of Rights
			3. **2012 FTC report**
				1. **Emphasized 3 areas**

**Privacy by design**: Companies should **promote consumer privacy throughout their organizations and at every stage in the development of their products and services**. They should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy

**Simplified consumer choice**: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company’s relationship with the consumer, or are required or specifically authorized by law. For practices requiring choice, **companies should offer the choice when the consumer is deciding about the data**. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected or (2) collecting sensitive data for certain purposes.

**Transparency**: Privacy notices should be **clearer, shorter and more standardized** to enable better comprehension and comparison of privacy practices. Companies should provide **reasonable access** to the consumer data they maintain; the extent of access should be **proportionate to** the **sensitivity** of the data and the **nature of its use**. All stakeholders should expand their efforts to **educate consumers about commercial data privacy practices**.

* + - * 1. **5 priority areas** for attention:

**do not track** mechanism

**mobile**

**data brokers**

**large platform providers** – comprehensive tracking

promotion of **enforceable self-regulatory codes**

* + - 1. Companies should obtain **express affirmative consent (opt in) before making material retroactive changes to privacy representations**
			2. **Annual Privacy and Data Security Updates**:
				1. **2015**: states reasonable data security practices include **at least 5 principles**

**Know the Data**: be aware of what consumer info they have and who has legitimate access to the data

**Limit Info**: limit info collected and maintained for legitimate business purposes

**Protection**: protect info by assessing risk and implementing security procedures and training

**Disposal** of information that’s no longer needed

**Remediation**: have plan in place to respond to security incidents

* + - * 1. **2016**: discusses various cases where consumers’ information was being collected without their knowledge, as well as 3 new technologies

**Smart TVs** (ability to track consumer viewing habits also expressed concern about apps that can be used to activate mic and listen for **audio beacons** emitted by TVs)

**Drones** (practical issues of providing choice and transparency)

National Telecommunications and Information Administration (NTIA) issued a report of best practices from its multi-stakeholder process concerning privacy, transparency and accountability issues for drones:

Show care when operating the drone or collecting and storing data

Limit the use and sharing of data

Secure data

Monitor and comply with evolving federal, state and local laws re drones.

**Ransomware** (steps businesses can take to prevent infiltration and limit impact)

* + - * 1. **2017**

Staff Report on **Cross-Device Tracking**: 4 recommendations

Transparency about practices

Offering choice to consumers about tracking

No cross-device tracking of sensitive topics (health, financial and children’s info)

Maintaining reasonable security

Workshop on Privacy and Security Issues Related to **Connected, Automated Vehicles**

* + - * 1. **2018**

**Recommendations to improve security updating process for mobile devices**

Educating the consumer on the need for installing updates should be a critical role for businesses, government and advocacy groups

Businesses should ensure that security updates for mobile devices continue for the time period consistent with the “consumers’ reasonable expectations”

Businesses should streamline the security-updating process

**Key Takeaways from “Connected Cars” Workshop**

Collection of data from consumers will likely lead to innovations that would benefit consumers, such as tailored entertainment choices, shorter commutes, and faster response times by emergency responders

Types of data collected will range from aggregate statistics to non-personal to sensitive personal information

Consumers will likely be concerned about unexpected secondary uses of their data

Connected cars will likely have cybersecurity risks that can be exploited by hackers to extort money or even cause physical harm

**Best practices** discussed included information sharing, network design, risk assessment and mitigation, and standard setting

* + - * 1. **2019**

June 2019 - FTC **finalized the Military Credit Monitoring Rule**, which requires **nationwide CRAs to provide free electronic credit monitoring services for active duty military consumers**.

July 2019 – FTC and DoJ announced **settlement with Facebook** – order imposed **$5 billion penalty** as well as modifications to first order, which are designed to change FB’s overall approach to privacy. **Largest penalty ever imposed on any company for violating consumers’ privacy**.

* 1. **INFORMATION MANAGEMENT FROM A U.S. PERSPECTIVE (18-22 QUESTIONS)**

Effective information management addresses legal and reputational risks while using information appropriately to meet the organization’s goals. Protection of privacy requires writing of policies that comply with applicable law and actual implementation. Increasingly important for US companies is compliance with laws and rules governing international data flows.

* + 1. **4 Basic Steps for Information Management** (**KNOW THESE STEPS IN DETAIL**)
			1. **Discover**: company’s environment, information privacy goals across depts, and corporate culture – the foundation for building company policies
				1. **Issue identification and self-assessment** – goals will serve as the foundation for the company’s policies.
				2. **Determination of best practices** – some standards are mandatory for members of a specific industry group
			2. **Build**: in view of goals, facilitate and restrict flow of PI where appropriate
				1. **Procedure development and verification** – close coordination between those writing the policies (legal and compliance) and IT experts and others who work in the various departments requiring policy compliance.
				2. **Full implementation**
			3. **Communicate**: effective communication to internal and external audiences; transparency critical
				1. **Documentation** – internal and external so that appropriate messages are made to relevant audiences.
				2. **Education** – internal audiences must be trained on policies and procedures with individual accountability for compliance; specific policies and general goals communicated to decision-makers and consumer-facing employees for appropriate messaging; written privacy notice must accurately reflect company policy to external audiences -> summary form that highlights key terms of the policy on top of longer, more detailed statement of privacy and security practices
			4. **Evolve**: constant evolution in response to changing tech, laws and market conditions – once established, info mgmt system must have process for review and update
				1. **Affirmation and monitoring**
				2. **Adaptation**
		2. **Data Sharing and Transfers** (practices and controls for managing PI)
			1. **Data inventory**: important for an organization to undertake an inventory of the personal information it **collects, stores, uses or discloses** – whether internally or externally. Include both customer and employee data records. Document data location and flow and evaluate how, when, and with whom the organization shares the information as well as the means used for data transfer. This inventory is legally required for institutions covered by the GLBA Safeguards Rule. Benefits include identification of risks that could affect reputation or legal compliance. Penalties likely less severe if company established system of recording and organizing its data inventory. Inventory should be reviewed & updated regularly.
			2. **Data classification**: classify data according to its **level of sensitivity – confidential, proprietary, sensitive, restricted and public**. Classification level defines clearance of individuals who can access or handle that data, as well as the baseline level of protection appropriate for that data. (Sensitive: e.g., personnel or customer records, trade secrets & business plans). More sensitive data can be segregated from less sensitive data through **access controls** that enable only authorized individuals to retrieve the data or by being kept in an entirely **separate system**. Holding all data in one system can increase the consequences of a single breach. In the US, classification is often important for compliance purposes because of sector-specific privacy and security laws - different rules apply to different categories of information (e.g., financial services information and medical information). Can also help with compliance audits for particular types of data, enable production only of necessary information, and enable cost-effective use of storage resources.
			3. **Data flow mapping**: After data inventoried and classified, data flow should be examined and documented. Map and document **systems, applications and processes** for handling data to **identify compliance gaps**.
			4. **Determining Data Accountability**.
				1. **Storage**: Where, how and for what length of time stored?

Laptop v desktop or centralized computer center

Limited retention periodsmitigate risk of loss from a breach

* + - * 1. **Sensitivity**

Data owner is responsible for assigning proper sensitivity level or classification based on company policy

Example: confidential, proprietary, sensitive, restricted (available to select few) and public (generally available)

* + - * 1. **Encryption**

No notice required for loss under many breach notification laws if sufficiently encrypted or protected by other effective technical means (in transit / at rest)

* + - * 1. **Transferability**: Transborder data flows? If so, how transferred?

Privacy requirements of origination and destination countries may not be the same

* + - * 1. **Governing Law**: Who determines rules that apply?

Controller/processor (GDPR), covered entity/business associate (HIPAA), service provider (GLBA)

* + - * 1. **Processing**: How processed and will processes be maintained?

Defined processes, Employee training

* + - * 1. **Dependency**: Is use of data dependent on other systems?

Working condition of those systems (e.g., cloud provider, special computer programs)? Outdated?

* + 1. **Privacy Program Development**
			1. **Risks of Improper Use of PI:** in designing and administering a privacy program, an organization should consider and balance four types of risk of using privacy information:
				1. **Legal risk**: Not complying with privacy laws and not fulfilling contractual commitments
				2. **Reputational risk**:damaging trust in the brand: organizations can face both legal enforcement and reputational harm if they do not adhere to their stated privacy policies
				3. **Operational risk**:affecting efficiency and inhibiting use of personal information that benefits the organization and customers
				4. **Investment risk**:hampering the ability of the organization to receive an appropriate return on its investments in information, IT and information processing programs
			2. **Privacy Policies and Disclosure**
				1. Privacy policies are central to information management programs – provide info and are important legal documents. If organization violates promise made in privacy policy communicated in a privacy notice, then FTC or state attorney general may bring enforcement action for deceptive practice.
				2. **Decision: One or Multiple Privacy Policies?** – one is better, avoid complications and conflicts in handling PI, which will inhibit sharing/cooperation w/in the organization
				3. **Policy Review and Approval**: organization should not finalize privacy policy w/o legal consultation followed by executive approval (avoid criticism for being too lax or reputational problems if too strict and can’t satisfy promises). Should tell employees and then current/former customers of changes to privacy policy through privacy notice. In 2012 report and 2015 update, FTC said companies should obtain express affirmative consent (opt-in) before making “material” retroactive changes to privacy representations – material change at minimum includes sharing customer info with 3rd parties after commitment at time of collection not to share.
				4. **Communicate Privacy Policy Through Notice**
				5. **Policy Version Control**: needs to be updated as info collection, use and transfer needs evolve. Should be reviewed periodically, and scheduled at least annually. Replacement must be systematic across all physical and electronic posting. Should reflect policy revision date + any version number. Save and store older versions for compliance / enforcement action purposes. Data used in compliance with the policy notice in effect when the data was collected unless data subject later agrees to terms of revised notice.
		2. **Managing User Preferences**: User should have right to consent to data collection and use. User should have right to opt-out of information being sold or shared with third parties. User should also have access to personal information held about them as well as ability to challenge accuracy of the data.
			1. **Opt-in: Affirmative Consent**
				1. **HIPAA** requires opt-in consent before PHI is disclosed to a 3rd party, subject to exceptions
				2. **FCRA** requires opt-in before a consumer’s credit report may be provided to an employer, lender or other authorized recipient.
				3. **Industry standards**: email marketers require a “double opt-in” or “confirmed opt-in”.
				4. **GDPR**- opt-in consent is appropriate for marketing
				5. **Sensitive Data**: Opt-in is preferred consent when collecting sensitive info such as customer’s geolocation data.
			2. **Opt-out (Consumer Choice**): Consent is assumed unless consumer specifically states otherwise
			3. **No Consumer Choice (No Option)**: Consumer should expect information to be shared with 3rd parties or used in other ways (e.g., third-party shipping, fraud prevention or first party marketing)
			4. **Challenges to Effective Management of User Preferences**
				1. **Scope**:an organization must decide how broadly an opt-out or another user preference will apply
				2. **Mechanism**: for providing an opt out can vary – the channel for marketing should be the channel for exercising a user preference
				3. **Linking**: a user’s interactions through multiple channels can be a management challenge when customers interact with an organization. If opt out is received through one channel, should implement this preference across other platforms
				4. **Time period**: for implementing user preferences is sometimes set by law (e.g., CAN-SPAM and TSR mandate specific time periods for processing customer preferences)
				5. **Third party vendors**: user preferences expressed by the first organization should be honored by the vendor
			5. **Customer Access and Redress**: APEC Principles provide guidance on proper scope of access requests and appropriate exceptions to providing access:

**Individuals should be able to**

1. Obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;

2. Have communicated to them, after having provided sufficient proof of their identity, personal information about them:

* within a reasonable time;
* at a charge, if any, that is not excessive;
* in a reasonable manner; and
* in a form that is generally understandable

3. Challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

**Such access and opportunity for correction should be provided except where:**

* + - * the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question;
			* the information should not be disclosed due to legal or security reasons or to protect confidential information; or
			* the information privacy of persons other than the individual would be violated.

If a request under (1) or (2) or a challenge under (3) is denied, the individual should be provided with reasons why and be able to challenge such denial.

* + 1. **Incident Response Programs Cyber Threats (e.g., ransomware)**: Training should cover not only how to protect information but also what to do if that information is compromised. An incident response program allows an organized approach to addressing and managing the aftermath of a security breach or cyber-attack, with a goal of limiting damage and reducing recovery time and costs.
			1. **Preparation**: Preparing users and IT staff to handle potential incidents
			2. **Identification**: determining whether an event is, indeed, a security incident
			3. **Containment**: limiting the damage of the incident and isolating affected systems to prevent further damage
			4. **Eradication**: finding the root cause of the incident and removing affected systems from the production environment
			5. **Recovery**: permitting affected systems back into the production environment and ensuring no threat remains
			6. **Lessons Learned**: completing incident documentation and performing analysis to learn from the incident and potentially improve future response efforts
		2. **Workforce Training**: once an organization has an information management program in place, it should provide regular training to its employees and keep records of who has been trained, especially those working with sensitive information, to ensure compliance and consistency. Training should be tailored to individual roles and responsibilities.
		3. **Accountability**: questions privacy professionals should ask when determining accountability: where, how and for what length of time should data be stored? How sensitive is the information? Should the information be encrypted? Will the information be transferred to or from other countries, and if so how? What are each country’s privacy laws? Who determines the rules that apply to the information? How will the information be processed, and how will these processes be maintained? Is the use of PI dependent upon other systems?
		4. **Data Retention and Disposal (FACTA)**: Businesses should have a written program outlining how to maintain and shred documents or destroy other data. This means that there is a well-defined, step by step procedure for various types of data and documents, including procedures for collecting and protecting the documents and data until the time that it is destroyed. Businesses should have retention schedules that mandate when records need to be securely destroyed. FACTA disposal rule requires businesses to take “reasonable measures” to protect against unauthorized access to or use of consumers’ information. FTC says burning, pulverizing, and shredding are all considered reasonable measures. The disposal rule is designed to be flexible, allowing anyone affected by the rule to choose which measures are “reasonable” based on costs and benefits of different disposal methods. Disposal rule allows use of document destruction contractors.
		5. **Online Privacy**: Companies do not need to provide choice before collecting and using consumers’ data for practices that are consistent with the context of the transaction, consistent with the company’s relationship with the consumer, or as required or specifically authorized by law. Don’t need to opt in to give delivery company shipping info.
			1. **Internet:** The transfer of “**packets**” and their unpacking and receipt facilitate speed but also result in privacy vulnerabilities.
			2. **Privacy Considerations for Online Information**
				1. **Threats to Online Privacy**

Unauthorized access,

Malware - software that has malicious purposes, i.e., unauthorized remote control of computer.

Phishing - tricks users into providing log-in credentials

Spear Phishing (phishing attack that is particularly aimed at the individual user… Ex: when an email appears to be from the user’s boss instructing the user to provide PI).

**Social Engineering** - attackers try to ***persuade*** a user to provide info or create some other security vulnerability. Usually by impersonating an employee, eavesdropping on private conversations, stealing ID.

**Technical attacks** – SQL injection, cookie poisoning, use of malware – attack exploits technical vulnerability or inserts malicious code

* + - * 1. **Online Security**
		- **Web Access**
			* Employees of the org should be trained in security and also anticipate that an attacker will utilize more than one method.
			* Website infrastructure are usually targeted because they are externally facing and easily accessible through web browsers.
			* **Strong security measures**: 2-factor authentication, e.g., manual password + token or ID card. Also, displaying the password field in HTML can mask the input characters with asterisks or bullets.
			* **Cookies** – imprecise means for authenticating and authorizing end-user access; can be deleted or blocked by the user, can’t differentiate individual users of same machine
		- **Data in Transit** - Transport Layer Security
			* TLS is the standard for PII encryption in transit, including end user verification info
			* TLS replaced SSL, which is no longer considered secure
		- **Protecting Online Identity**
			* be smart with **login/passwords/PINs**, install antivirus/firewall **software**, be cautious when using **Wi-Fi networks or Bluetooth** (prone to interception and very vulnerable), **file sharing** - limit directory access on P2P file sharing applications (BitTorrent), **public computers**, **public charging stations** (USB ports may contain malware), **websites** (if insecure don’t provide sensitive info).
		- **Mobile Online Privacy**
			* New privacy and security issues presented by Mobile devices

**Geolocation data**- hard to anonymize location data because it tracks people from work to the home and allows linkage of location data with identity.

Rules for collection/use/storage - location based advertisements.

**Location Based Services (LBS)** will likely expand as it presents many benefits to local businesses

* + 1. **Privacy Notices**: A “privacy notice” is a description of an organization’s information management practices. They’re for **consumer education** and **corporate accountability**. Tells the individual what information is collected, how the information is used and disclosed, how to exercise any choices about uses or disclosures, and whether the individual can access or update the information.
			1. **Purpose**: Effective online privacy notice provides consumers with easy-to-follow guidance about how their information is being accessed, used and protected. Regulators and courts often treat privacy notices as enforceable against a company.
			2. **Privacy Statement should include**:
				1. Effective date
				2. Scope of notice
				3. Types of personal information collected (both actively and passively)
				4. Information uses and disclosures
				5. Choices available to the end user
				6. Methods for accessing, correcting or modifying personal information or preferences
				7. Methods for contacting the organization or registering a dispute
				8. Processes for communicating policy changes to the public
			3. **TrustArc recommends**:
				1. Say what the organization does and do what is stated
				2. Tailor disclosures to the actual business operations model
				3. Do not treat privacy statements as disclaimers
				4. Revising the privacy statement frequently to ensure it reflects current business and data collection practices
				5. Communicate these privacy practices to the entire company
			4. **Trustmark**: images or logos that are displayed on websites to indicate that a business is a member of a professional organization OR to show that it has passed security and privacy tests – designed to give consumers confidence in safety of e-commerce. TrustArc, Norton and BBB are examples of trustmarks
			5. **Methods for Communicating Notices**: make it accessible online, in places of business, provide updates and revision (GLBA requires customers of financial institutions to receive the privacy notice annually), ensure the appropriate personnel are knowledgeable about the policy.
				1. **Layered Notices**

Made as an alternative to single long notice. Basic idea is to offer “layers” that provide key ideas and allow readers the option to read further detail with “clickthrough”

Short notice is top layer and summarizes the notice.

Full notice is bottom layer and provides the complete privacy notice for those interested in reading it.

“Just in time” notice - “at or before the point of information collection”

* + - * 1. **Mobile Privacy Notice**: small screens make notice challenging, FTC has recommended best practices – overarching principles to address privacy and security on mobile devices include:
* Privacy by design (PbD) or privacy by default
* Transparency
* Simplification of consumer choices
	+ - * 1. **Customer Access to Information**: no general legal right for individuals in US to access or correct personal information held about them

HIPAA governs access to and correction of PHI under the Privacy Rule

FCRA governs access to and correction of PI for credit, employment or similar

**Collection and Use of E-Data**

Active Data Collection - end user deliberately provides info to the website through its input mechanism

Passive Data Collection - occurs when info is gathered automatically as user navigates from page to page - often without end user’s knowledge (*cookies, mechanisms to ID device*, etc.)

To maximize privacy and reduce exposure in the event of a data breach, web forms should be designed to require only the information that is genuinely needed and should make it clear to the end user what, if anything, is optional.

Autocomplete function of most web form submission processes should be disabled (or at least masked with asterisks or other obscuring characters) so that sensitive personal information is not exposed on shared computers (such as a machine used jointly by multiple family members for surfing the web).

To protect against account access by an unauthorized person, passwords should not be prepopulated in a web form.

**Third-Party Interactions**

Identity of websites being blurred through the emergence of *syndicated content* (not created by host site), *web services* (facilitate communication b/w computers), *co-branded sites* (info sharing b/w partners permitted if disclosed in privacy notice), *web widgets* (apps that can be installed on a page), and *online advertising networks* (connect online advertisers with web publishers that host ads on their site).

Must understand 3rd party interactions and ensure proper privacy protection in place.

If technically feasible, end users should understand which entities are capturing or receiving PI and each entity must accept accountability for legal obligations

**Onward Transfers to Third Parties**: FTC considers onward transfer to be the responsibility of the host website - not the 3rd party - and has issued guidance and brought enforcement actions toward this end

3rd Party that receives data from collecting entity falls into 1 of 3 categories:

processes data on behalf and at direction of collecting entity

receives data for completion of collecting entity’s transaction, such as to ensure payment, delivery

receives data and independently determines how to use it to further its own purposes (e.g., marketing) -> effectively become controllers

*Processor* (in EU) = *business associate* for HIPAA (healthcare industry) = *service provider* for GLBA (financial industry)

* + 1. **Vendor Information Management**:
			1. **Vendor Contracts**: contracts with vendors should include provisions for privacy and security of data handled or processed by the vendor, such as:
				1. Confidentiality provisions
				2. No further use of shared information
				3. Use of subcontractors
				4. Requirement to notify and to disclose breach
				5. Info Sec provisions
				6. End of relationship
			2. **Vendor Due Diligence**: standards for selecting vendors should include:
				1. **Reputation** and past history - prior security incidents, references
				2. **Financial condition and insurance** – sufficient resources in case of a breach/litigation
				3. **Information security controls** – sufficient controls in place to avoid loss or theft
				4. **Point of transfer** – potential security vulnerability, ensure secure transfer between parties
				5. **Disposal of information** – appropriate destruction for any format/media
				6. **Employee training and user awareness** – established system
				7. **Vendor incident response** – established protocols with required cooperation to meet goals/objectives
				8. **Audit rights** – monitor to ensure compliance with contract (periodic assessments / reports by independent 3rd party)
			3. **Vendor Incidents**: if a vendor data breach incident occurs, vendor should have a response program in place that is communicated to the contracting entity. Cooperation between the two entities should aim to meet the business and legal needs of the contracting entity, which is ultimately responsible for the actions of its vendor.
			4. **Cloud Issues**: contracts with cloud vendors should include confidentiality provisions, information security provisions, prohibit further use of shared information, require subcontractors to follow privacy and security protection terms in vendor’s contract, require notification of data security breaches
		2. **International Data Transfers**
			1. **U.S. Safe Harbor and Privacy Shield**: agreement included commitments by US companies, detailed explanations of US laws, and commitments by US authorities. US companies wishing to import personal data from the EU under the Privacy Shield accepted obligations on how that data could be used, and those commitments were legally binding and enforced through DoJ. **Both are now invalid (*Schrems I and II*)**.

***Schrems II***: Held that data transfers under US Privacy Shield from the EU to the US are now illegal and data exporters that wish to continue transferring personal data to the US must use other data transfer mechanisms

* + - 1. **Binding Corporate Rules (BCRs)**: additional basis for transferring data, providing that a multinational company can transfer data between countries after certification of its practices by an EU privacy supervisory agency. **Internal** **rules** which define the internationalpolicy in **multinational** group of companies or **international organizations** regarding **intra-organizational cross-border** **transfers of personal data**
			2. **Standard Contractual Clauses**: where a company contractually promises to comply with EU law and submit to the supervision of an EU privacy supervisory agency
			3. **Other Approved Transfer Mechanisms**:
				1. Codes of conduct
				2. Certification mechanisms
				3. Data protection seals and marks
				4. Adequacy decisions of the data protection authority
				5. Consent of the data subject
		1. **Other Key Considerations for U.S.-Based Global Multinational Companies**
			1. **General Data Protection Regulation (GDPR)**

|  |  |
| --- | --- |
| **GDPR Requirements** | **Data Subject Rights Under GDPR** |
| * New requirements for processors
* Notification of security breaches
* Designation of data protection officers
* Accountability obligations
* Sanctions of up to 4% of worldwide revenues
* Rules for international transfers
 | * Right to be Informed
* Right of Access
* Right to Rectification
* Right to Erasure (Right to be Forgotten)
* Right to Restriction of Processing
* Right to Data Portability
* Right to Object
* Right Not to be Subject to Automated Decision-Making
 |

1. **Key Terms**

**Personal Data**: any data that relates to identified or identifiable natural person. Data that is deidentified, encrypted, or pseudonymized remains personal data if can be used to reidentify person. Data is ***only*** considered “**anonymized**” **if** process used is **irreversible**.

First and last name

Home address

Email address including first and last name

Identification card number

Location data

IP address (often not PII in US)

Cookie ID (often not PII in US)

Advertising identifier on phone

Data held by doctor or hospital, ***even if separated from patient’s name***

**Sensitive Personal Data**: sensitive personal data requires business to obtain **“explicit consent”** from person to process the data **for a specified purpose** unless exception applies

Race or ethnic origin

Political opinions

Religious or philosophical beliefs

Trade union membership

Genetic data

Biometric data

Health data

Sex life or sexual orientation

**Data Subject**: any natural person whose data is being collected, stored or processed.

**EU- entity** + process data of **data subject non-EU** 🡪 **GDPR** rights apply

**Non-EU entity** + monitoring behavior or targeting goods/services of **EU data subject** 🡪 **GDPR** rights apply

**Controller**: entity that directs processing of data to further its business objectives (i.e., determines the purposes and means of processing personal data). Obligations include:

Implement data protection by default and by design

Provide instructions to processors

Ensure data security

Report data breaches

Cooperate with DPAs

Appoint a DPO for the business

Identify legal basis for processing

Maintain data processing records

Conduct data protection impact assessments (DPIAs)

**Processo**r: entity that processes personal data on behalf of controller. Requirements flow down to sub-processor. Obligations include:

Compliance with instructions of controller

Confidentiality

Record of processing activities

Data security

Data breach reporting

Cooperation with DPAs

**Consent**: freely given, specific, informed, and unambiguous indication of data subject’s wishes expressed by statement or clear affirmative action. **Valid *informed* consent** requires entity to provide data subject with the following:

Controller’s identity

Purpose of processing for which consent is sought

Types of data that will be collected

Information about the right to withdraw consent

Information about automated processing

Risks of transfers outside Europe

**Data Protection Authority (DPA)**: independent public authorities that investigate and enforce data protection laws at the national level and provide guidance on interpretation of those laws. One DPA in each EU Member State with the exception of Germany, which has a *federal DPA* with jurisdiction over the *public sector* and *16 Lander (or state-level*) DPAs with jurisdiction over the *commercial sector*.

**Data Protection Officer (DPO)**: primary point of contact on data protection issues within business based in EU. DPO facilitates and reviews GDPR compliance. DPO must have expertise in data protection law relevant to entity’s data processing. DPO must not have any conflicts of interest, that is, DPO must not have duties related to processing personal data that conflict with duties related to monitoring compliance. **If company does not have EU presence** **must appoint EU representative** – someone who is subject to enforcement proceedings under GDPR. Whether a DPO is needed does not depend on status as controller or processor.

Are data subjects from EU?

Is data in/from EU?

Large-scale monitoring of data subjects?

Large-scale processing of sensitive PI?

Where is entity based?

1. **General Principles**: 7 key principles

**Lawfulness, fairness and transparency**: Entity should

have legal basis for processing personal data, data subjects should be made aware of rules, safeguards and risks associated with their data

make processing transparent to data subjects so understand extent of processing –communications (including privacy notices) must be concise, easily accessible and written using clear and plain language that is easy to understand

**Purpose limitation**: personal data must be collected for specified, explicit and legitimate purposes that are clearly expressed to data subjects. “What” and “why” need to be known before personal data collected. No further processing (such as storage) in a manner that’s incompatible with the original purpose of collection.

Further processing for archiving purposes in the public interest, scientific or historical research purposes *or* statistical purposes *not incompatible* with the original purposes and is permitted under GDPR.

**Compatibility of further processing depends on**:

Relationship between purposes of collection and purposes of further processing

Nature of personal data and safeguards adopted to ensure fair processing

Reasonable expectations of data subjects and impact of further processing on data subjects

**Data minimization**: Processing must be adequate, relevant and limited to what is necessary considering purposes of processing – if no longer necessary should be deleted or anonymized and any data retention period should be limited to strict minimum.

**Accuracy**: personal data must be accurate and up to date – every reasonable step taken to ensure that inaccurate personal data are erased or rectified w/o delay

**Storage limitation**: personal data kept no longer than necessary for the purposes of processing – linked to minimization. Data retention period should reflect purposes of processing, legal obligations and industry best practices.

***Entities should establish time limits to review or erase stored personal data to ensure kept only as long as necessary***

**Integrity and confidentiality**: Appropriate technical or organizational measures must be taken to ensure level of security appropriate to risk of processing personal data, considering *state of the art*; the *costs of implementation*; and the *nature, scope, context and purposes* of processing as well as *risk* (likelihood and severity) *to rights and freedoms* of individuals

**Accountability**: Controller responsible for and must be able to demonstrate compliance with the previous 6 principles

1. **Data Subject Rights**: providing data subjects with control over their personal data. Controllers must respond to requests w/in 1 month of receipt (or, where necessary, w/in 3 months), in writing or, if requested, orally. Identity of requestor should be verified using reasonably measures (e.g., photo ID). Controller cannot charge fee *except* to cover admin costs for manifestly unfounded or excessive requests or for additional copies of info previously provided. Controller can refuse to comply w/ request *if* exemption exists or it’s manifestly unfounded or excessive.

**Right to be Informed** of Transparent Communication and Information: Controllers must provide **privacy notice**

**Layered approach** - short overview of key info linking to additional layers of detailed info

**Just in Time** notices – info relevant to personal data about to be collected

**Privacy Dashboards** – info and privacy preference mgmt. in centralized area

**Right of Access**: right to obtain from controller: confirmation whether processing data subject’s personal data, copy of personal data, and other information that should already be provided in privacy notice. Called a subject access request– allows data subject to understand what, why, and how regarding processing and verify lawfulness of the processing. Right of access, given scope of info, is often the **gateway to exercise of rights under GDPR**.

**Right to Rectification**: controller must confirm accuracy of personal data – data subject has right to have inaccurate personal data corrected and, considering purposes of processing, to have incomplete personal data completed, which may be done via supplementary statement

**Right to Erasure (Right to be Forgotten)**: For valid request, controller must delete relevant personal data, including from backup systems, unless an *exemption* applies, such as processing necessary to comply with legal obligation or establishment, exercise or defense of legal claim. Where controller makes personal data available online, controller must use reasonable measures to inform other controllers processing the personal data to erase any links to or copies of the personal data. **Right to erase applies where**:

personal data are no longer necessary … [for] purposes for which collected or otherwise processed

data subject withdraws consent … and there is no other legal ground for the processing

data subject objects to processing [based on legitimate interests] and no overriding legitimate grounds for processing”

personal data have been unlawfully processed

personal data have to be erased for compliance with legal obligation

personal data have been collected … [to offer] information society services [to children] (i.e., online services offered to children; e.g., online shops, live or on-demand streaming services, and companies providing access to communication networks)

**Right to Restriction of Processing**: right to limit the way personal data is processed – marking of stored personal data with aim of limiting processing in future. Examples for methods of restriction include temporarily moving data to another system, making personal data unavailable to users or removing data from website. ***Controllers required to communicate rectification or erasure of personal data and any restriction of processing to each recipient to whom they have disclosed the personal data***, unless this is impossible or involves disproportionate effort. Required information for such communications should be documented in the record of processing activities. **The right applies where**:

Accuracy of personal data contested, and controller is verifying the accuracy

Processing is unlawful and data subject prefers to restrict use of personal data rather than erase it

Controller no longer needs personal data, but data subject requires it for establishment, exercise or defense of legal claims

Data subject objected to processing, and controller is verifying whether its legitimate grounds override those of data subject

**Right to Data Portability**: allows data subject to port data to themselves or to another controller. May request data in structured, commonly used, and machine-readable format. Right to data portability cannot adversely affect rights and freedoms of others, including trade secrets or intellectual property rights. The right *only applies*

to **personal data provided by the data subject** (actively and knowingly provided by the data subject **or** observed data provided by the data subject through the use of the service or device such as search history or location data)

where the processing based on **consent or performance of a contract**, AND

the **processing carried out by automated means**

**Right to Object**: allows data subject to require controllers to stop processing personal data (e.g., for direct marketing purposes). Controller must cease all such processing, including any related profiling activities.

**Data subject may object on any of the following legal bases**:

a task carried out in the public interest

exercise of official authority, or

legitimate interests

But **not an absolute right**: data subject must provide reasons why objecting to processing and **controller can refuse the request if**

compelling legitimate grounds overriding those of data subject OR

processing is necessary for establishment, exercise or defense of legal claims

**Right Not to be Subject to Automated Decision-Making**: applies w/o any action by data subjects (like right to be informed). This right is a general prohibition on fully automated decision-making, including profiling, that has a legal or similarly significant effect (e.g., cancellation of K). Controller cannot carry out such processing unless decision is

necessary for performance of contract between data subject and controller

authorized by law (e.g., monitoring and preventing fraud) OR

based on data subject’s explicit consent

1. **Breach Notification and Response**:

**Data Breach** means breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (broader than under most US laws)

GDPR authorizes **fines for data breach up to 4%** of worldwide revenues

**Notice Required from Controllers**: to relevant DPA w/in **72 hours after discovery** of breach – a reasonable degree of certainty that security incident compromised personal data. If deadline can’t be met – must provide reasons for delay. Notification not required if unlikely to result in risk to rights and freedoms but still must document details of breach (e.g., nature of breach, personal data affected, likely consequences of breach, remedial measures taken, decision whether to report to DPA)

**Notice Required from Processors**: required to notify controllers without undue delay after discovery of breach. Controller should strongly consider including specific instructions for how to handle notice requirement in K between controller and processor.

**Notice to Data Subjects**: If data breach is likely to result in high risk to individuals’ rights and freedoms, controller must notify affected data subjects without undue delay.

At a minimum, **notification must be in “clear and plain language”** and must include:

Name and contact of DPO (or appropriate person)

Likely consequences of the data breach

Any measures taken by controller to mitigate breach

**Controller exempted** from notifying data subjects when

risk of harm low because affected data is protected (such as encrypted data)

controller has taken steps to protect data subject from harm (such as suspended accounts) AND

notice would impose disproportionate effects on controller (and would still require public notice of breach).

1. **Enforcement**: With significant fines imposed, EU data protection law is a compliance program (not just aspirational)

**Complaint Process**: Administrative complaint can be initiated by data subject by filing it with a DPA or by a DPA. Data subject can also file complaint in courts in the EU Member States where alleged issue occurred, where data subject resides, or where data subject works. DPA can impose administrative fine. Data subject can appeal DPA decision to a national court. Additionally, data subject has right to seek judicial remedy against controller or processor in Member State where controller or processor is established or where data subject has habitual residence.

**Liability for Compensation**: both controller and processor can be liable to data subjects for harm caused by unlawful processing of personal data

Controllers liable for damages caused by unlawful processing. Processors liable for processing in violation of GDPR obligations on processors and for processing in violation of instructions given by the controller

If controller and processor involved in same processing, each is liable for the entire damage. Once data subjects have been fully compensated, controller or processor entitled to compensation from other relevant parties corresponding to their part in responsibility for damage.

Where there are joint controllers, each controller is liable for the entire damage. Once data subjects have been fully compensated, controllers involved can bring proceedings to recover portions of damages from each other.

Both controllers and processors are **exempt** from liability when not in any way responsible for event giving rise to damage.

**Level of Fines**: GDPR has **two levels of fines**. Higher-level fines can be up to 4% of global annual revenues. Lower-level fines can be up to 2% of global annual revenues.

**Higher-level fines** focus on basic principles of processing (consent, lawfulness of processing, and processing special categories of data), rights of data subjects, and transfer of personal data to recipient outside EU. Max fines are the greater of €20M or 4% of global annual revenues

**Lower-level fines** relate to integrating data protection by default to by design, records of processing, cooperation with DPAs, security of processing data, notification to DPAs of data breach, communication of data breach to data subjects and designation of a DPO. Max fines can be greater of €10M or 2% of global annual revenues

Additionally, **Member States can impose criminal sanctions** for violations of GDPR

1. **Global Data Flows**: GDPR has strict rules concerning European data traveling to a third country

**Requirements for Data Transfers**: Transfers of personal data from the EU, Norway, Liechtenstein and Iceland (i.e., the European Economic Area (EEA)) to non-EEA countries or international organizations are **prohibited unless one of the following transfer mechanisms can be relied upon**. A transfer of personal data does not include personal data merely in transit from one EEA country to another EEA country via a non-EEA country.

**Adequacy Decision**: Personal data is permitted to flow freely to countries that have adopted legal protections that EU law deems “adequate.”

**Deemed Adequate**: Andorra, Argentina, Canada (commercial communications only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay

**Less than full adequacy decision from European Commission**: US and Canada – permitted to transfer data only under certain defined circumstances

Data transfers are **prohibited** to countries without an adequacy decision **unless** the transfer is subject to **appropriate safeguards** or a **derogation applies**

**Appropriate Safeguards** include the following:

A legally binding and enforceable **instrument between public authorities** or bodies

**Binding corporate rules**

**Standard data protection clauses** adopted by European Commission

Standard data protection clauses adopted by a DPA and approved by European Commission

An approved code of conduct, together with binding and enforceable commitments of the non-EEA controller or processor

An approved certification mechanism together with binding and enforceable commitments of the non-EEA controller or processor

Contractual clauses authorized by DPA of controller or processor transferring the data outside of the EEA

Administrative arrangements between public authorities authorized by DPA in the country from which the transfer is being made

**Derogations [exceptions]**: conditions under which a transfer may occur – allow for transfer if **data subject has provided explicit consent to the transfer** OR if **transfer is necessary for**:

The performance of a contract between the data subject and controller (including pre-contractual measures) and the transfer is occasional

The performance or conclusion of a contract concluded in the interest of the data subject between the controller and a third party and the transfer is occasional

Important reasons of public interest

The establishment, exercise or defense of legal claims and the transfer is occasional or

The protection of the vital interests of an individual incapable of giving consent or

None of the above apply and the transfer is necessary for compelling, legitimate interests and the DPA is notified of the transfer

**Transfers from EU to US**: See pp. 15-16 above.

**EU-US Privacy Shield** – invalidated by Schrems II

**Standard Contractual Clauses (SCCs)**:

**Binding Corporate Rules (BCRs)**:

* + - 1. **APEC Privacy Framework (2004)**: The APEC Privacy Framework is a set of principles and implementation guidelines created to establish effective privacy protections that avoid barriers to information flows and ensure continued trade and economic growth in the APEC region of 27 countries. Non-binding agreement between Pacific coast members in Asia and the Americas.
				1. Contains **9 Information Privacy Principles** that **generally mirror the OECD Guidelines** but are more explicit about exceptions.

**Purpose: Preventing Harm**; recognizing the individual’s’ legitimate expectations of privacy, protection should be designed to prevent the misuse of personal information; remedial measures should be proportionate to the likelihood and severity of the harm posed by such collection.

**Notice**: controllers should be able to provide clear and easily accessible statements about their practices and policies at the time of collection or as soon after as is practicable; no notice is required where the information is publicly available.

**Collection Limitation**: limited to the relevant purposes of collection through lawful and fair means

**Uses of Personal Info**: only to fulfill the purpose of the collection except: where consent is provided; where necessary to provide a service or product requested by the individual; or by authority of law.

**Choice**: mechanisms to exercise choice regarding collection, use and disclosure

**Integrity of Personal Info**: info should be accurate, complete and kept up to date to the extent necessary for the purposes of its use

**Security Safeguards**: should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the info, and the context in which is held, and should be subject to periodic review and reassessment.

**Access and Correction**: individual should have access to the collected information, be able to challenge its accuracy, have the data corrected EXCEPT where burden or expense is unreasonable or disproportionate to the individual’s privacy; should not be disclosed due to legal or security reasons or to protect confidential info; or where the privacy of other persons would be violated.

**Accountability**: Personal information controller should be accountable for complying with these principles.

* + - * 1. The APEC Privacy Framework set in motion the process of creating the APEC **Cross-Border Privacy Rules (CBPR) system**.

**CBPR System**: The CBPR system has been formally joined by the United States, Canada, Japan and Mexico. The CBPR program is analogous to the EU-U.S. Privacy Shield in that both provide a means for self-assessment, compliance review, recognition/acceptance and dispute resolution/enforcement. Requires designation by each country of a data protection authority (the U.S. enforcement authority is the FTC). APEC CBPR system requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices must be assessed as compliant with minimum program requirements of APEC CBPR system by an accountability agent (the only U.S.-based accountability agent  is TRUSTe) and be enforceable by law. CBPR system does not displace or change a country’s domestic laws and regulations. CBPR system intended to provide a minimum level of protection if there are no domestic privacy protection requirements.

* + 1. **Resolving Multinational Compliance Conflicts**
			1. **EU Data Protection Versus E-Discovery**: there’s a conflict between U.S. pretrial e-discovery and EU data protection - transfer to the US of e-records is possible without consent once an ‘adequate’ level of protection is guaranteed whether that be by resorting to Standard Contractual Clauses, falling within the scope of a Safe Harbor agreement or by respecting Binding Corporate Rules
				1. Determine whether there is any potential framework to compel cooperation with US discovery rules. For example, under the **Hague Convention** or other bilateral agreements (depending on the civil or criminal nature of the request).

Production of transborder data may also be avoided by invoking the **Hague Convention on the Taking of Evidence**. Under the treaty, the party seeking to displace the Federal Rules of Civil Procedure bears the burden of demonstrating that it is more appropriate to use the Hague Convention and must establish that the foreign law prohibits the discovery sought. **Aerospaciale v. S.D. of Iowa** outlines factors that an American court may use to reconcile the conflict. These factors include:

importance of the documents or data to the litigation at hand

specificity of the request

whether the information originated in the United States

availability of alternative means of securing the information

extent to which the important interests of the United States and the foreign state would be undermined by an adverse ruling

* + - * 1. Consider whether any protected data is likely to be involved
				2. Consider whether a blocking statute or other local legal restriction or interpretation on data disclosure exists
				3. Investigate processes and options that respect the fundamental rights of European citizens

Redacting or anonymizing all documents in country, prior to disclosure and transfer to US

Privacy log

Trusted 3rd party

1. **LIMITS ON PRIVATE-SECTOR COLLECTION & USE OF DATA (20-24 QUESTIONS)**
	1. **CROSS-SECTOR FTC PRIVACY PROTECTION (2-4 QUESTIONS)**
		1. **The Federal Trade Commission Act**: power to prevent unfair methods of competition, deceptive acts or practices, seeking monetary redress, prescribing trade regulation rules, and establishing requirements
		2. **FTC Privacy Enforcement Actions**: FTC’s enforcement has evolved from focusing on “deceptive trade practices” to requiring the implementation of best practices in privacy and security (“fair trade practices”)
			1. **Deceptive practice** – involves material statement or omission likely to mislead consumers who are acting reasonably under the circumstances (e.g., false promises, misrepresentations, and failures to comply with representations made to consumers, such as statements in privacy policies)
		3. **FTC Security Enforcement Actions**: FTC has sanctioned companies for unfair trade practices when they failed to implement adequate ***protection measures for sensitive personal information*** or when they provided ***inadequate disclosures to consumers***.
		4. **The Children’s Online Privacy Protection Act of 1998 (COPPA)**: FTC is the rule making and enforcement agency. Requires **verifiable express consent from a parent before a child’s (under 13) PI is collected.**
			1. **Purpose**: primary goal of COPPA is to place parents in control over what information is collected from their young children online
			2. **Scope**:
				1. Applies to **operators of commercial (not nonprofit) websites and online services** (any service available over the Internet or that connects to Internet of WAN) (including mobile apps and IoT devices, such as smart toys), or on whose behalf such information is collected or maintained (such as when personal information is collected by an ad network to serve targeted advertising) **directed to children** **under 13** that ***collect, use, or disclose*** ***PI from children***.
				2. Website or online service may be deemed directed to children even if Terms of Service prohibits children from using the site or service
				3. Applies to operators of **general audience websites or online services** **with actual knowledge** that they are collecting, using, or disclosing PI from children under 13, and to websites or online services that have actual knowledge that they are collecting PI directly from users of another website or online service directed to children.
				4. Does not apply to info about kids collected online from parents or other adults - only applies to PI collected online from kids, including PI about themselves, their parents, friends, or other persons
				5. Applies even if kids volunteer PI and are not required by the operator to input the info
				6. Applies to operators that allow kids to publicly post PI
				7. “**Collection” includes passive tracking** of kid’s PI thru persistent identifier and not just active collection
				8. Kids between 13-18 are NOT protected under COPPA – State AGs have focused attention on privacy rights of middle and high school students.

**Multistate enforcement action by State AGS** who alleged that requesting middle school and high school students to fill out **surveys** that appeared to be meant for colleges or universities when, in fact, the PI of the students was collected for advertisers, and soliciting educators in connection with the collection of the information was a **deceptive trade practice** under their respective **state consumer protection laws**.

* + - * 1. **Does not prevent** kids from **lying** about their age – covers operators with actual knowledge

Operators **NOT required to ask age** of visitors to their site – **but** if operator later learns that kid accessed the site, notice and parental consent requirements are triggered

* + - * 1. **Foreign-based websites** and online services **must comply with COPPA if** they are directed to children in the US, or if they knowingly collect personal information from children in the U.S.

U.S.-based sites and services that collect information from foreign children also are subject to COPPA

* + - 1. **Targeted to Children**: FTC looks at the following to determine whether a website or online service is targeted to children:
				1. Subject matter
				2. Age of models
				3. Visual and audio content used
				4. Language used
				5. Whether the site uses animated characters and children’s activities and incentives
			2. **Personal Information Defined as**:
				1. First and last name;
				2. A home or other physical address including street name and name of a city or town;
				3. Online contact information;
				4. A screen or username that functions as online contact information;
				5. A telephone number;
				6. A Social Security number;
				7. A **persistent identifier** that can be used to recognize a user over time and across different websites or online services (e.g., customer number held in a cookie, an IP address, a processor or device serial number, or a unique device identifier that can be used to recognize a user over time and across different websites or online services);
				8. A photograph, video, or audio file, where such file contains a **child’s image or voice**;
				9. **Geolocation information** sufficient to identify **street name and name of a city or town**; or
				10. Information concerning child or parents of that child that the operator collects online from the child **combined with** an identifier described above.
			3. **Requirements**
				1. Post a **clear and conspicuous privacy notice** describing PI practices **for info collected from kids** on the **homepage** of the website and a **functioning link to the privacy notice** on every page where PI is collected
				2. **Privacy Policy must include**:

Contact information for the website operators collecting/maintaining information

The type of information collected

How the information will be used

Whether the information will be disclosed to third parties and, if so, the general purpose of the third party, as well as a description of its business and acknowledgement of confidentiality

An option to consent to collection w/o consenting to disclosure to 3rd parties

A statement that child's participation will not be conditioned on the disclosure of more info than reasonably necessary to participate in the online activity.

A statement that the parent can review their child’s personal information, direct its deletion, and refuse to allow any further collection or use of the child’s information, and the procedures to do so

* + - * 1. Provide **direct notice to parents** about the site’s information collection practices
				2. Obtain ***verifiable parental consent*** before collecting personal information from children

**General rule**: any parental consent mechanism “must be ***reasonably calculated***, in light of available technology, ***to ensure that person providing consent is the child's parent***”.

**Acceptable** *verifiable parental consent*:

If using PI for **internal purposes**:

**“Email Plus”** method – send an email to the parent containing the required notice and request that the parent provide consent by responding in an email.

Take additional, confirmatory step after receiving the parent’s email, e.g., after a reasonable time delay, send another email to the parent to ***confirm consent*** and let parent know that s/he can revoke consent if they wish. May also request in initial email that parent include phone number or mailing address in reply so that you can follow up to confirm via phone or postal mail

If disclosing children’s **PI to third parties / making it publicly available** through such activities as a chat room, message board, personal home page, pen pal service, or email service:

A **more reliable method** – provide a form for the parent to sign and mail or fax back to you; ask a parent to use a credit card in connection with a transaction (perhaps a fee just to cover the cost of processing the credit card); maintain a toll-free telephone number staffed by trained personnel for parents to call in their consent, **or** you can accept emails from parents where those *emails contain a digital signature* or *other digital certificate that uses public key technology*.

Acceptable validation method for parental consent where child’s info disclosed to 3rd party: parent can provide consent by signing emailed consent form and mailing it back (**print-and-send method)**.

Knowledge-based identification/authentication (e.g., out-of-wallet information, dynamic multiple-choice challenge questions)

Facial recognition technology – face match to verified photo ID (encryption and prompt deletion afterward)

* + - * 1. **Exceptions** that allow an operator to collect a child’s name and e-mail address:

If it is being **collected along with the parent’s e-mail address for** purposes of providing the required **notice and obtaining consent**

To respond **once to a specific request** from a child, ***as long as the e-mail address is deleted immediately*** after responding

**Multiple-contact exception**: To respond more than once to a specific request of a child, as long as, after the first communication with the child, the **operator must make reasonable efforts to ensure parent receives appropriate notice** to provide an opportunity for the parent to opt-out of the information collection and order the operator to delete the e-mail address and stop contacting the child.

Note – if notice to parent is unable to be delivered, deemed to be lack of reasonable efforts

To collect a child’s name and e-mail address where necessary to protect the **safety of a child participating on the site or online service**. The operator must give notice to the parent, use it only for such safety purpose and not disclose it on the site or service.

To collect a child’s name and e-mail address for the sole purpose of **protecting security or integrity of the site,** take **precautions against liability,** respond to **judicial process** or for law enforcement on a matter related to **public safety**.

* + - * 1. Provide **parents a choice** as to whether their children’s PI will be **disclosed to third parties**
				2. Provide **parents access and opportunity to delete** the children’s PI and **opt-out** of future collection or use the information
				3. **Not condition a child’s participation** in a game, contest, or other activity on the child’s disclosing more PI than is reasonably necessary to participate in that activity
				4. Maintain the **confidentiality, security, and integrity** of PI collected from children
			1. **Enforcement**
				1. FTC enforcement actions and civil penalties up to $43,280 per violation
				2. **No private right of action** under COPPA. States may bring civil actions under COPPA, but **COPPA preempts state law**
			2. **California**
				1. **California’s Privacy Rights for California Minors in the Digital World** (“Online Eraser Law”)

Individuals **under 18** have the **right to request removal** of info that they’ve posted online

**Prohibits online advertising to minors** of products that minors are **not legally permitted to buy** (e.g., alcohol, tobacco & firearms) and also restricts certain online advertising practices based on the minor’s PI

Requires the Operators to **issue notices to minors** who are registered users **of right to remove** or to request and obtain removal **of content or information posted by that minor** registered user.

Requires the Operator to **provide clear instructions to minors** who are registered users about how to remove, or request and obtain removal of, such content or information **and notify** such minors that **removal does not ensure complete or comprehensive removal** of the content or information posted on the Operator’s site

* + - * 1. **CCPA (2020)**: prohibits selling PI of California consumers under 16 w/o appropriate consent. For teens 13-15, permits businesses to obtain affirmative (opt-in) consent directly from minor.
			1. **Delaware’s Online and Personal Privacy Protection Act of 2016 (DOPPA)**
				1. prohibits online advertising to minors related to products these consumers are not legally permitted to buy (i.e., alcohol, tobacco, firearms dietary supplements and sexually explicit material) and also restricts certain online advertising practices based on the minors’ personal information.
				2. Delaware law defines a minor as a **state resident under the age of 18**.
				3. Also applies to websites not necessarily directed to minors, but also to websites known to be frequented by minors
				4. Privacy policies must be conspicuously posted
				5. Acknowledging that 3rd parties do not have a right to know viewing habits of e-book users without informed consent absent special compelling circumstances, DOPPA **prohibits e-book services from disclosing PII of readers to 3rd parties unless certain exceptions apply,** such as law enforcement or by court order
			2. **GDPR**: restriction on processing data of children under 16 unless valid consent obtained from parent or guardian
		1. **Future of Federal Enforcement** (Data brokers, Big Data, IoT, AI, unregulated data):
			1. **Data Brokers**: Harvest and monetize personal data w/o consumer knowledge or consent. No federal law covers marketing use of consumer data.
				1. **Vermont**: 1st data broker law in US. The law only affects third-party data handlers – those trafficking in the data of those with whom they have no association – as opposed to ‘first-party’ data handlers like Facebook, Google or Amazon, which harvest data directly from their users. The law requires (1) annual registration with Vermont Secretary of State, including certain disclosures regarding practices related to the collection, storage or sale of consumer PI, along with consumer ability to opt out, and disclosure of any breaches; and (2) maintenance of minimum data security standards for commercial actors. It also prohibits any individual or business from acquiring brokered PI through fraudulent means for the purpose of stalking, harassment, ID theft, discrimination or fraud. Enforced by State AG pursuant to state unfair and deceptive practices act. Private right of action under credit reporting laws.

**Data broker** means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the personal information of a consumer with whom the business does not have a direct relationship.

Sharing creates a large web of data exchanges, which makes it virtually impossible for a consumer to determine the originator of a particular data element.

* + - * 1. **California**: The CCPA “define[s] a data broker as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” The data broker amendment requires data brokers to register with the California AG or face potential fines. It also requires that the AG create a publicly available registry of data brokers.
			1. Big Data:
			2. Internet of Things:
			3. Artificial Intelligence:
			4. Unregulated Data:
	1. **HEALTHCARE** **(5-7 QUESTIONS)**
		1. **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**: **No preemption** of stricter state privacy laws, and the California Medical Information Privacy Act (CMIA) expands health information privacy protection duties to providers of software, hardware, and online services. HIPAA applies to **covered entities** and, since HITECH and HHS’s final rule in 2013, the HIPAA privacy and security rules are codified and apply directly to **business associates**, making them directly liable for violations. Health information in the hands of other persons or entities is not protected by HIPAA. Compared with other US privacy laws, HIPAA is most detailed implementation of Fair Information Privacy Practices (FIPPs). **HIPAA permits use and disclosure of PHI for treatment, payment and healthcare operations as well as for medical research**.
			1. **Protected health information (PHI)**: any individually identifiable information held by a covered entity or its business associate that is created, collected, transmitted or maintained by a covered entity and relates to a past, present or future health status (physical or mental condition, provision of health care, or payment for healthcare) of that individual. PII + PHYSICAL OR MENTAL HEALTH OR OTHER HEALTH CONDITION = PHI.
			2. **ePHI**: any PHI transmitted or maintained in electronic (storage) media. Paper records, paper-to-paper fax transmissions, and voice communications (e.g., telephone) are not considered transmissions via electronic media.
			3. **Covered Entities**:
				1. **Healthcare providers** that conduct certain transactions in electronic form
				2. **Health plans** (health insurers)
				3. **Healthcare clearinghouses** (3rd party host orgs that handle or process medical info)
			4. **Business Associates**: Any person or organization, other than member of covered entity’s workforce, that performs services and activities for, or on behalf of, covered entity, if such services or activities involve use or disclosure of PHI.
			5. **can enforce directly against BA only for the following**:
				1. Failure to provide HHS with records and compliance reports, cooperate with complaint investigations and compliance reviews, and permit access to info (including PHI) to determine compliance
				2. Retaliatory action against person for filing HIPAA complaint, participating in investigation or other enforcement or opposing unlawful act or practice under HIPAA
				3. Failure to comply with Security Rule
				4. Failure to provide breach notification to CE or another BA
				5. Impermissible use or disclosure of PHI
				6. Failure to disclose copy of ePHI to CE, individual or individual’s designee (whichever specified in BAA) to satisfy CE’s obligations regarding form, format, and time & manner of access
				7. Failure to make reasonable efforts to limit PHI to minimum necessary to accomplish purpose of the use, disclosure or request
				8. Failure to provide accounting disclosures
				9. Failure to enter BAA with subcontractors that create or receive PHI on their behalf and failure to comply with implementation specifications for BAA
				10. Failure to take reasonable steps to address material breach or violation of subcontractor’s BAA
			6. **HIPAA Privacy Rule**: **Goal is implementation of policies and procedures to prevent, detect, contain and correct security violations**. Privacy Rule includes standards and implementation specifications that encompass administrative, technical and physical safeguards. Some “required” and some “addressable” (i.e., assess whether appropriate for adoption and, if not, document why not reasonable and, if appropriate, adopt alternative measure).

**Key Privacy Protections**

* + - * 1. **Privacy notices-** requires a covered entity to provide a detailed privacy notice at the date of first service delivery
				2. **Authorizations for uses and disclosures-** the notice authorizes the use and disclosure of PHI for essential healthcare purposes: treatment, payment and operations (TPO), and other established compliance purposes. **Other uses or disclosures of PHI require the individual’s opt-in authorization**
				3. **“Minimum Necessary” use or disclosure-** other than for treatment, covered entities must make reasonable efforts to limit the use and disclosure of PHI
				4. **Access and accountings of disclosures-** individuals have the right to access a **copy** of their own PHI from a covered entity or a business associate. Have a right to receive an **accounting of** certain **disclosures** of their PHI that have been made, a reasonable charge may be assessed, and right to **amend** PHI possessed by a covered entity
				5. **Safeguards-** covered entities implement administrative, physical, and technical safeguards to protect the confidentiality and integrity of all PHI.
				6. **Accountability-** covered entities must designate a privacy official who is responsible for the development and implementation of privacy protections.
				7. **Does not apply to information that has been de-identified** (remove 18 identifiers listed in the rule, or have an expert certify the risk of re-identifying is very small).Research is permitted on de-identified information.
			1. **HIPAA Security Rule**: establishes minimum security requirements for PHI that a covered entity receives, creates, maintains or transmits **in electronic form**. Strives for “reasonable level” of security not perfect security. Permits covered entity to “use any security measures that allow the CE or BA to reasonably and appropriately implement the standards and implementation specifications.”
				1. **Covered Entities and Business Associates Must**:

Ensure the confidentiality, integrity, and availability of all ePHI a covered entity creates, receives, maintains or transmits

Protect against any reasonably anticipated **threats or hazards** to security or integrity of ePHI

Protect against any reasonably anticipated **uses or disclosures** of ePHI that are **not permitted or required** under the Privacy Rule

Ensure compliance with the Security Rule by its workforce

* + - * 1. **Covered Entities Must**:

Identify **privacy official** who is responsible for the implementation and oversight of the security rule compliance program (may be the same person who’s doing the privacy rule compliance program)

Conduct **initial and ongoing risk assessments** (accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity)

Implement a **security awareness and training program** for its workforce

* + - 1. **Disclosures to Law Enforcement**: Disclosure to law enforcement is permitted pursuant to **court order** or **grand jury subpoena**, or through an **administrative request**, **if 3 criteria are met**:
				1. Information sought is **relevant and material to a legitimate law enforcement inquiry**
				2. Request is **specific and limited in scope** to the extent reasonably practicable in light of the purpose for which the information is sought
				3. **De-identified information could not reasonably be used**

In cases of conflicting laws, disclosure permitted when “required by law,” even if disclosure does not otherwise fit within the law enforcement or other exception.

* + 1. **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009**: Enacted as part of the American Recovery and Reinvestment Act of 2009 to **promote the adoption and meaningful use of health information technology**
			1. **Notice of Breach**: covered entities and business associates have burden of proof that impermissible use or disclosure did not constitute a breach. If there’s a high probability that security or privacy of information was compromised, covered entity **must notify individuals within 60 days** after discovery. Business associate must notify covered entity. If breach affects **more than 500 people**, covered entity must **notify HHS** **immediately**, if **more than 500 in same jurisdiction**, must **notify the media**. All breaches requiring notice must be reported to HHS at least annually.
			2. **Increased penalties**: Penalties up to $1.5M for the most willful violations and extends criminal liability to individuals who misuse PHI.
			3. **Limited Data**: Limited data set refers to PHI from which “facial” identifiers are removed (i.e., 18 identifiers **except** dates (e.g., admission, discharge, service, DOB, DOD); city, state, zip code; and age in years, months or days of hours). **Limited data sets are still PHI**. Limited data set + data use agreement permits disclosure to 3rd party for research, public health or health care operations w/o patient authorization. All disclosures by a covered entity should attempt to comply with the definition of a limited data set. If not feasible, data disclosed must be the minimum amount necessary. Patients who directly pay their provider for medical care may restrict their PHI from being disclosed to health plan unless disclosure otherwise required by law.
			4. **Electronic Health Records**: Providers who make meaningful use of Electronic Health Records can qualify for funding created by HITECH. **Sharing through EHRs with other entities can only be done with patient consent**. Covered entities must provide individuals with copy of EHR on request and must account for all non-oral disclosures made within 3 years on request. Covered entities may not sell EHRs without consent of patient and covered entities cannot receive payment for certain marketing plans.
			5. **Genetic Information and Nondiscrimination Act 2008 (GINA)**: created new national limits on use of genetic information in health insurance and employment.
				1. **Health Insurance Companies**: prohibits **discrimination on basis of genetic predispositions** in the absence of manifest symptoms **OR** **requesting that applicants receive genetic testing**
				2. **Group Health Plan Providers**

prohibits adjusting **premiums** or other contribution schemes on **basis of genetic information**, absent manifestation of disease or disorder

prohibits **requesting or requiring** **genetic testing** in connection with offering group health plans with **exception** for requests for **voluntary research testing**

* + - * 1. **Employers**: prohibits discrimination in **employment decisions** based on genetic information **OR** because **family member has manifested genetic disease**. Employers can’t require, request or purchase genetic information about employee or family member unless exception applies. **Exceptions**:

request is inadvertent

request is part of **employer-offered wellness program** that employee voluntarily participates in with written authorization

as part of family medical history request made to comply with Family and Medical Leave Act (FMLA) of 1993 or state of local leave laws of certain employer leave policies

employer purchases commercially and publicly available materials that include the information

as part of **genetic monitoring** required by law (e.g., for toxin exposure in workplace) **or** where employee voluntarily participates with written authorization

employers who conduct DNA analysis for law enforcement purposes as a **forensic lab** or for identifying human remains

* + - * 1. **If Exception Applies**: employers (and unions) that legitimately possess genetic info must keep it on **separate forms** in **separate medical files**, and the files must be **treated as confidential employee medical records**
				2. **Penalties**: Statutory penalty of $100/day/participant for noncompliance
				3. **Enforcement**: **No private right of action** but, depending on violation, private right of action may be available under the underlying laws that it revised (e.g., ERISA, Social Security Act, Civil Rights Act) as well as state laws for disparate treatment (overt discrimination). GINA does not provide for a cause of action for disparate impact (i.e., fair in form (facially neutral) but discriminatory in operation – employer avoids liability by claiming the challenged practice or policy is “job-related” and consistent with “business necessity”; that is, no other way to achieve employer's legitimate goals).
		1. **The 21st Century Cures Act of 2016**: purpose is to accelerate medical product development and move from bench to bedside faster and more efficiently (e.g., research process for new medical devices and prescription drugs, quicken process for drug approval, and reform mental health treatment). Promotes interoperability of disparate EHRs, adoption of EHRs and support for human services. Seeks a balance between protection of personal data and public interest in appropriate utilization of the information. Attempts to balance conflicting goals of privacy vs need for medical and genetic research. Promotes precision medicine and improving health IT w/r/t nationwide interoperability and minimizing information blocking.
			1. **Low-risk medical devices**: FDA barred from regulating mobile health apps designed to maintain or encourage healthy lifestyle if unrelated to diagnosis, prevention or treatment of disease.
			2. **Certain individual biomedical research information exempted from disclosure under FOIA**: To the extent that individual biomedical research information could reveal individual identity, the Cures Act exempts this information from mandatory disclosure under FOIA
			3. **Researchers permitted to remotely view PHI**: Allows medical researchers to remotely view PHI but must meet minimum safeguards consistent with HIPAA
			4. **Information blocking prohibited, but HIPAA’s protection of PHI remains**: prohibits health care providers, health IT providers, health information exchanges, or networks from information blocking (unreasonable conduct likely to interfere with the exchange of electronic health information). Violation of information-blocking provision of Cures Act can result in fine up to $1M per incident.

**8 Exceptions to Information Blocking**:

* + - * 1. Preventing harm
				2. Privacy
				3. Security
				4. Infeasibility
				5. Health IT performance
				6. Content and manner
				7. Fees
				8. Licensing
			1. **Certificates of confidentiality for research**: provides stronger privacy protections for those participating in research, particularly those with alcohol and substance abuse issues. Requires certificates of confidentiality to be issued by NIH for any federally funded research and permits NIH to issue certificates at its discretion for research that is not federally funded.
			2. **Compassionate sharing of mental health or substance abuse information with family or caregivers**: requires HHS to issue guidance to HIPAA regarding circumstances under which health care provider or covered entity permitted to discuss with family members or caregivers treatment of adult with mental health disorder or alcohol or substance abuse disorder
		1. **Confidentiality of Substance Use Disorder (SUD) Patient Records Rule (42 CFR Part 2)**: Several decades before passage of HIPAA. Entities subject to rule are likely to also be subject to HIPAA Privacy Rule. In many areas, these two requirements will have parallel requirements. Should review both to understand when the two do not converge. **No preemption** of stricter state laws.
			1. **Scope**: covers disclosure and use of “patient identifying” information by treatment programs for alcohol and substance abuse. The rule restricts use of any information, whether written or verbal, that could lead to or substantiate criminal charges against a patient concerning their alcohol or drug usage.
			2. **Applicability**: applies to any program that **receives federal funding**. “**Program**” is individual or entity who **holds itself out as providing (and provides) alcohol or substance abuse diagnosis, treatment or referral for treatment**. Does not include “general medical facility” – **unit** within a general medical facility wd be a program though and so wd **medical personnel** or other staff in a general medical facility whose **primary function** is diagnosis, treatment, etc. If not covered program, HIPAA and state law may still provide rights.
			3. **Disclosure**: program must obtain written patient consent before disclosing information subject to the rule
			4. **Re-disclosure**: re-disclosure of info obtained from a program is **prohibited if** information would identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment.
			5. **Exceptions to consent for disclosure**: internal communications, medical emergencies, scientific research, audits and evaluations, communications with qualified service org (QSO) to provide services to the program, crimes on program premises or against program personnel, child abuse reporting, and special court order (subpoena, general court order, search warrant, or official request ***is not enough*** for law enforcement to access treatment information).
			6. **Security of records**: entity lawfully holding patient-identifying information must have formal policies and procedures in place to protect security of information. Separate requirements for paper and electronic records. Violations are a crime. 1st offense is max $500. Subsequent is max $5,000. **Violations reported to U.S. Attorney’s Office**.
			7. **42 CFR Part 2** (Revised July 2020): serves to protect patient records created by federally assisted programs for treatment of **substance use disorders (SUD)**. Patients need the right to access treatment without worrying that their records will be used to take away their children, housing, employment, insurance, public benefits, or freedom. Part 2 revised to further facilitate better coordination of care in response to opioid epidemic while maintaining confidentiality protections against unauthorized disclosure and use.
			8. **Part 2 vs HIPAA**: Both protect patient privacy by regulating how patient information can be shared and disclosed. HIPAA applies to many types of patient information, not just SUD information, and is less protective of patient privacy than Part 2. ***Unlike HIPAA***, **Part 2’s privacy protections (1) no exception to written consent for TPO; (2) only special court order w/r/t civil or criminal proceedings; and (3) follow the records** **even after they are disclosed** – the recipient of the records is now bound by Part 2’s privacy and security requirements for the Part 2 records. When SUD info disclosed with consent, must include written statement that info cannot be re-disclosed.
	1. **FINANCIAL (5-7 QUESTIONS)**
		1. **The Fair Credit Reporting Act of 1970 (FCRA)**: enacted in 1970 to regulate the consumer reporting industry and provide privacy rights in consumer reports. **First federal law to regulate use of personal information by private businesses**.
			1. 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.
			2. Regulates any **consumer reporting agency (CRA)** that furnishes a “consumer report,” which is used primarily for assisting in establishing consumer’s eligibility for credit. CRA is any person or entity that **compiles or evaluates personal information** **for the purposes of furnishing consumer reports to third parties** **for a fee**. (Experian, Equifax, and TransUnion). In 2017 Equifax breach, no FCRA violation because Equifax had not furnished the stolen data to the hackers.
			3. **Consumer Report**: any communication by a CRA related to an individual that pertains to the person’s
				1. Creditworthiness
				2. Credit standing
				3. Credit capacity
				4. Character
				5. General reputation
				6. Personal characteristics
				7. Mode of living

and is used as **a factor** in **establishing eligibility** for **credit, insurance, employment or other business purpose**.

* + - 1. **Users of consumer reports must meet 4 main requirements under FCRA**
				1. 3rd party data for substantive decision making must be appropriately **accurate,** **current and complete**
				2. **consumers must receive notice** when 3rd party data is used to make adverse decisions about them
				3. consumer reports may be used **only for permissible purposes**
				4. **consumers must have access** to their consumer reports and an **opportunity to dispute them or correct** any errors.
			2. **FCRA also specifically requires CRAs to**
				1. provide consumers with access to the information contained in their consumer reports and the opportunity to dispute any inaccurate information
				2. take reasonable steps to ensure the max possible accuracy of information in the consumer report
				3. not report outdated negative information
				4. provide consumer reports only to entities that have a permissible purpose under the FCRA
				5. maintain records regarding entities that received consumer reports
				6. provide consumer assistance as required by FTC rules.
			3. **Enforcement**: enforcement available through **dispute resolution, private litigation and govt actions**. If not satisfied with dispute resolution process of CRA, individuals have a private right of action, with recent trends leaning toward class actions. Noncompliance with the FCRA can lead to civil and criminal penalties. In addition to actual damages, violators subject to statutory damages max $1,000 per violation, and max $4063 per willful violation. **Govt enforcement actions by FTC & CFPB (shared), concurrent with State AGs** (individually or collectively by multiple states). State AG must give notice to FTC before filing suit and FTC retains right to intervene. **Limited preemption** of state law.
			4. **Notice Requirements under FCRA**: FTC published a notice to all users of consumer reports of obligations under the FCRA.
				1. Users must have **permissible purpose** to obtain consumer report.

ordered by a court

instructed by the consumer in writing

for the extension of credit after application from a consumer

for employment purposes with consumer’s consent

* + - * 1. User must provide **certifications** to show permissible purposesand only use reports for that permissible purpose
				2. Users must **notify consumers when adverse actions are taken**
				3. Users must **securely dispose of consumer report data**
			1. **FCRA** requires disclosure by all persons who use credit scores in making or arranging loans secured by residential real property.
			2. **Consumer Reports & Employment**: FCRA imposes additional obligations on organizations that intend to use consumer report information for employment purposes. **Employee investigation** of suspected misconduct or noncompliance with laws are not treated as consumer report **if**
				1. Employer or its agent **complies with the procedures** in the act
				2. **No credit information** is used
				3. A **summary describing the nature and scope** of the inquiry is **provided to employee** **if** **adverse action** is taken based on the investigation
			3. **Investigative Consumer Reports**: contain information about a consumer’s character, general reputation, personal characteristics, and mode of living, which is obtained through **personal interviews** (e.g., with neighbors, friends, associates or acquaintances of the employee, such as reference checks) **by an entity or person that is a CRA** – consumers have special rights under FCRA.
				1. **User of the report must disclose its use to consumer subject to the following**:

Consumer must be informed that an investigative consumer report may be obtained.

Disclosure must be in writing and must be mailed or otherwise delivered to consumer some time before but not later than 3 days after date on which report first requested.

Disclosure must include statement informing consumer of rights to request additional disclosures of nature and scope of investigation and summary of consumer rights required by FCRA. Summary of consumer rights provided by CRA that conducts investigation.

User must certify to CRA that required disclosures made and that user will make necessary disclosure to consumer.

Upon written request of consumer within reasonable period after required disclosures, user must make complete disclosure of nature and scope of investigation in written statement mailed or otherwise delivered to consumer no later than **5 days after** date on which request received from consumer **or** report first requested, whichever is later.

* + - 1. **Medical Information**: FCRA limits use of medical info obtained from CRAs other than payment info that appears in coded form and does not identify the medical provider. **If report to be used for** **employment** purposes, consumer must provide specific written consent and the medical info must be relevant.
			2. **Prescreened Lists**: Creditors & insurers permitted under FCRA to obtain limited consumer report info for use in connection with firm unsolicited offers of credit or insurance under certain circumstances – (1) before offer made, must have established criteria that will be relied on to the make the offer and (2) maintain the criteria on file for 3 years starting on date offer is made.
		1. **The Fair and Accurate Credit Transactions Act of 2003 (FACTA)**: Further **amended the FCRA**. **Preempts state laws in most areas**. Required **truncation** of credit and debit card numbers, so receipts don’t show full number. Gave consumers new rights to an **explanation of their credit scores**. Gave individuals the right to request **free annual credit report** from each of the 3 national consumer credit agencies. Required regulators to promulgate:
			1. **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 consumer information in a way that prevents unauthorized access and misuse of the data. **Disposal standard requires practices that are** **“reasonable” to protect against unauthorized access to or use** of the consumer data. Reasonableness includes consideration of sensitivity of the info being disposed of, cost/benefit of disposal methods & available technology.
				1. **Enforcement by FTC, federal banking regulators and CFPB**. Violations subject to civil liability and federal and state enforcement actions. FI’s subject to both FACTA Disposal Rule and GLBA Safeguards Rule should incorporate disposal practices into info sec program mandated by Safeguard Rule.
				2. **Acceptable, reasonable measures** include developing and complying with **policies to**:

**Burn, pulverize or shred** papers containing consumer report information so that the information cannot be read or reconstructed

**Destroy or erase electronic files or media** containing consumer report information so that the information cannot be read or reconstructed

**Conduct due diligence and hire a document destruction contractor** to dispose of material specifically identified as consumer report information consistent with the rule

* + - 1. **Red Flags Rule**: requires certain ***“financial institutions” and “creditors”*** to develop and implement written identity theft detection programs that can identify and respond to “red flags” that signal identity theft.
				1. “**Financial institution**” is all banks, savings and loan associations and credit unions.
				2. “**Creditor**” is any entity that in the **ordinary course** of its business **regularly**:

gets or uses consumer reports in connection with credit transactions

furnishes information to consumer reporting agencies in connection with credit transactions **or**

advances money to or on behalf of a person

Does **not** apply to entities that extend **credit only for expenses incidental to a service** (e.g., doctors, attys, healthcare providers)

Applies to entities that extend **credit to consumers** **without using consumer reports** to make credit decisions (i.e., required to implement a “Red Flag” program to detect and deter identity theft)

* + - * 1. Detection program must include **4 basic elements** that create a framework to deal with the threat of identity theft:

**Reasonable policies and procedures to identify red flags of identity theft** that may occur in day-to-day operations. Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. If an ID doesn’t look genuine, it’s a “red flag”.

**Incorporate identified flags into the program so it’s designed to detect them**. If fake IDs are identified as a red flag, for example, must have procedures to detect possible fake, forged, or altered identification.

**Spell out appropriate actions** when a red flag is detected.

**Update the program regularly to reflect changes in risk level and new threats**.

* + - * 1. Authorizes regulations for application of the rule **to businesses whose accounts are “subject to a reasonably foreseeable risk of identity theft**.”
				2. The rule **does not provide a checklist for specific red flags that must be included** in identity theft detection programs. Each FI or creditor is required to **develop its own list of red flags**. Examples: alerts, notifications or warnings from a consumer reporting agency; suspicious identification documents; suspicious personal identifying data; and unusual use of a covered account.
		1. **The Financial Services Modernization Act of 1999 (“Gramm-Leach-Bliley” Act or GLBA)**: applies to **financial institutions** (any company **significantly engaged** in providing **financial products or services**). Financial institutions are required to **securely store** personal financial information, **provide notice** of their policies regarding the sharing of personal financial information, and provide consumers with the **choice to opt out of sharing** some personal financial information. Prohibits FIs from disclosing consumer account numbers to nonaffiliated companies for the purposes of telemarketing and direct mail marketing, even if the consumer has not opted out of sharing the information for marketing purposes.
			1. **Scope**: applies to banks, non-bank lenders, financial advisors, check-cashing services, payday lenders, real estate appraisers, tax preparers, mortgage brokers, ATM operators, colleges and universities that issue student loans
			2. **GLBA Privacy Rule**: GLBA’s privacy protections generally apply to “consumers” (in particular, subset called “**customers**” – consumers with whom entity has ongoing relationship) or individuals **who obtain financial products or services** from a financial institution to be used **primarily for personal, family or household purposes**. Financial services companies who don’t have “customers” are not subject to some of GLBA’s requirements, such as those related to notice.
				1. Under privacy provisions, **FIs must**:

**Securely store** personal financial information

Provide **notice of their data sharing policies** regarding personal financial information

Provide consumers with the **choice to opt out** of sharing some personal financial information

* + - * 1. **Scope**: GLBA regulates financial institution management of **nonpublic personal information**, defined as **personally identifiable financial information**:

provided by a consumer to a financial institution

resulting from a transaction or service performed for the consumer, or

otherwise obtained by the financial institution.

**Excluded** from the definition are **publicly available information** and any **consumer list derived without using personally identifiable financial information**.

* + - * 1. **Enforcement**: Banking and related financial institutions that fail to comply with GLBA requirements can be subject to substantial penalties under Financial Institutions Reform, Recovery and Enforcement Act (FIRREA). FIRREA penalties range from max $5,500 for violations of laws and regulations to a max $27,500 if violations are unsafe, unsound or reckless and as much as $1.1M for “knowing” violations. **No preemption** of state laws under GLBA, but validity of stricter state laws can be challenged due to limited preemption under FCRA – courts wd need to determine which federal financial privacy statute governs for a particular state law. ***No private right of action*** but failure to comply with certain notice requirements can be deceptive trade practice enforceable by state and federal authorities. ***CFPB has enforcement authority for GLBA Privacy and Safeguards Rules***. State AGs can enforce GLBA.
				2. **Privacy Notices**: FI’s **must**

Prepare and provide to customers **clear and conspicuous notice** of the financial institution’s **information-sharing policies and practices** (initial and annual), which must include:

What information is collected

With whom the information is shared

How it’s protected

A reasonable opt-out process, with opt-outs processed w/in 30 days

**If notice standard met**:

FI may share any info it has with its **affiliated companies and joint marketing partners** (i.e., other FIs with whom the entity jointly markets a financial product or service) **and consumer reporting agencies**

FI may share consumer info with **nonaffiliated companies and other 3rd parties**, but only **after** **notice and** **opportunity to opt-out**

Comply with regulatory standards established by certain government authorities to protect the security and confidentiality of customer records and information and protect against security threats and unauthorized access to or certain uses of such records or information.

* + - * 1. **No Opt-Out Required** for the following:

FI shares information with 3rd party that provides essential services like data processing or servicing accounts if ensure that info not used for any other purpose

Disclosure is legally required

FI shares customer data with 3rd party service providers that market the FI’s products or services if ensure that info not used for any other purpose

Disclose to CRA

* + - 1. **GLBA Safeguards Rule**: requires FIs to develop and implement **comprehensive information security program** that contains administrative, technical and physical safeguards **to protect security, confidentiality, and integrity** of customer information (electronic and paper).
				1. **3 Levels of Security for Consumer Info**:

**Administrative** security, which includes program definition, management of workforce risks, employee training, and vendor oversight.

**Technical** security, which covers computer systems, networks, and applications in addition to access controls and encryption.

**Physical** security, which includes facilities, environmental safeguards, business continuity, and disaster recovery.

* + - * 1. **Reasonably Designed To**:

ensure the security and confidentiality of customer information

protect against anticipated threats or hazards to security or integrity of information

protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to customer

* + - * 1. **GLBA-Compliant Info Sec Plan**: Rule allows **flexibility for “appropriately implemented security measures,”** but must:

Designate 1 or more employees responsible for info security and coordination of safeguards

Identify and assess risks to customer information in each area of FI’s operations

Evaluate effectiveness of safeguards in place to protect information against identified risks

Design and implement safeguards program that is regularly monitor and tested

Use service providers who are required by contract to maintain appropriate safeguards

Evaluate and adjust program on ongoing basis as circumstances change, including changes in business arrangements or operations, or results of testing and monitoring of safeguards

* + - 1. **State Requirements regarding Financial Privacy & Security**: GLBA does not preempt state laws
				1. **California SB-1 (California Financial Information Privacy Act (CFIPA))**: expands financial protections afforded by GLBA. Increases disclosure requirements and grants consumers increased rights with regard to sharing of information. Written **opt-in consent required** for FI to share personal information with **nonaffiliated 3rd parties**. Opt-in provisions must be presented **on a form titled “important privacy choices for consumers”** and be written in **simple English**. Consumers have right to **opt-out** of sharing with **affiliates not in same line of business**. FI does not need consent to share nonmedical info w/wholly owned subs in same line of business (insurance, banking or securities) if regulated by same functional regulator. **Statutory damages**: negligent noncompliance $2500 per consumer to max $500K per violation. Willful noncompliance – no cap.
				2. **New York** **Department of Financial Services (NYDFS) Cybersecurity Regulations (2017)**: comprehensive and strict cybersecurity regs for FIs. NY is **1st state to go this far beyond GLBA**. **Regs are** **in line with NIST Cybersecurity Framework** and cover banks, credit unions, investment companies, licensed lenders, mortgage brokers, life insurance companies, savings & loan associates.

**FI must implement cybersecurity program with the following**:

risk assessments

documentation of security policies

designation of a chief information security officer (CISO)

limitations on data retention

incident response plan

audit trails

**Differences from GLBA**:

**Nonpublic info** **defined more broadly than GLBA**’s personally identifiable financial information

**Key requirements not in GLBA related to** - personnel, reporting obligations, documentation obligations, and obligations regarding 3rd party service providers

* + 1. **Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010**: Title X of this act **created the Consumer Financial Protection Bureau (CFPB)** as an independent bureau **within the Federal Reserve**.
		2. **Consumer Financial Protection Bureau (CFPB)**: Oversees relationship between consumers and providers of financial products and services. ***Assumed rule-making authority under existing laws relating to financial privacy and other consumer issues (FCRA, GLBA and Fair Debt Collection Practices Act)***
			1. **Enforcement Authority** over all non-depository FI and all depository institutions > $10 bn in assets
			2. For depository financial institutions with $10 bn or less, promulgates rules enforced by banking regulators
			3. CFPB regulates and enforces **unfair, deceptive or abusive acts and practices (UDAAPs)** (cf. FTC and State AGs enforcement against “unfair and deceptive” acts and practices)
				1. **Abusive act or practice**:

**Materially interferes** with **ability of consumer to understand term or condition** of a consumer financial product or service; or

Takes **unreasonable advantage** of:

* + - * + A **lack of understanding by the consumer** of the material risks, costs or conditions of the product or service
				+ The **inability of a consumer to protect its interests** in selecting or using a consumer financial product or service; or
				+ The **reasonable reliance by the consumer** on a covered person to act in the interests of the consumer.
			1. **Enforcement**
				1. Conduct **investigations** and issue **subpoenas**
				2. Hold **hearings**
				3. Initiate **civil actions** against offenders
			2. **Penalties for Violations**
				1. **Civil penalties from** $5,526/day for federal consumer privacy law violations, $27,631/day for **reckless** violations and $1,105,241/day for **knowing** violations
				2. State AG’s can also bring civil actions to enforce law or regulations
		1. **Online Banking**: addressing concerns related to online banking requires combo of measures by FI (design & updates of software) and consumer education.

**FIs should take the following steps**:

* + - 1. carefully choose operating system
			2. select appropriate internet browser
			3. use firewalls, antivirus programs, and anti-malware programs
			4. authentication - employ strong passwords and encryption
	1. **EDUCATION (0-2 QUESTIONS)**

Education records for institutions that receive **federal funding** have privacy protections under U.S. Law. Grades, disciplinary actions and other school info about a student deserve privacy protection.

* + 1. **Family Educational Rights and Privacy Act of 1974 (FERPA) (aka**: The Buckley Amendment): provides students with control over access and disclosure of education records (e.g., grades and behavior info). **Applies to all educational institutions that receive federal funding** (elementary, secondary and post-secondary). Violations can result in loss of federal funding for the educational institution. Intended to establish minimum federal standard for education records confidentiality and access. **No private right of action. No preemption**.
			1. **4 Requirements - Students have right to**
				1. **Notice of rights** under FERPA (annually)
				2. **Consent** (right to control the disclosure of education records to others)

must be signed (by hand or electronically), dated and written

must identify records to be discloses, purpose of disclosure and to whom disclosure is being made

* + - * 1. **Access, Review and Correction** of their own education records – school must provide records w/in 45 days after request

Access, inspect and review their personal info held by their school

Request corrections or updates to their personal info

Request hearing if request to correct or update is denied

* + - * 1. **Security and accountability**

Students and parents are given option to opt-out or block release of directory info

SSNs (or student ID numbers in some situations) are excluded from directory info

File complaints with the U.S. Department of Education

* + - 1. **Education record** means **all records** that are **directly related to student** and **maintained by or on behalf of a school**, including financial aid records and disciplinary records
				1. **Exceptions** (i.e., NOT education records)

campus police records

employment records

treatment or health records (i.e., records of student holder of FERPA rights that are ***made, used or maintained*** by healthcare provider ***only in connection w/treatment of student)*** so long as not disclosed for purposes other than treatment

If disclosed by school for ANY purpose other than treatment (including under any exception to FERPA’s general consent requirements), no longer excluded from “education records” and are subject to FERPA

If treatment records transferred to HIPAA covered entity for purposes of treatment, then the records become subject to HIPAA

applicant records of those who are not enrolled

alumni records

sole-possession records (e.g., created by faculty or staff for personal use)

grades on peer-graded papers before collected and entered into course instructor’s grade book.

* + - 1. **PII** includes
				1. Student’s name
				2. Name of student’s parent or other family members
				3. Student or student’s family’s address
				4. Personal identifiers such as SSN or student number
				5. Other identifiers such as D.O.B
				6. Other info that alone or in combo would link to the student
				7. Info requested by person whom school reasonably believes knows identity of student to which education record is linked
			2. **Holder of FERPA rights**
				1. **Student**: if 18 or older or any age if in college only
				2. **Parent** if student is a minor and in HS or HS + college classes
				3. **Parent w/o Student Consent**: if student is a dependent on parents’ taxes, regardless of age
			3. **Disclosure** of education records **permitted w/o consent if one of following** met:
				1. **Not personally identifiable**
				2. **Directory information** when release not blocked by student (opt-out requirement, unlike rest of FERPA)

defined by FERPA to include information that would not generally be considered an invasion of privacy or harmful if disclosed (e.g., name, date of birth, address, email address, telephone number, field of study, and honors received)

educational institution can declare information directory information and begin using it as such only after student provided an opportunity to opt out, or block, release of directory information

SSN cannot be directory information

student ID # cannot be directory information ***if*** it can be used to access education records without factor known only to authorized user (e.g., password or other authentication method not included in directory information)

* + - * 1. **Consent** by FERPA rights holder
				2. **Disclosure to FERPA rights holder**
				3. **Statutory exception** applies (e.g., health/safety emergency)
				4. **Permitted recipients w/o consent**:

School officials w/ “legitimate educational interest”

**Educational technology companies** are often designated as “school officials” under FERPA – contract with school can designate the company as a school official

Other educational institutions

Financial aid organizations

Researcher for studies on behalf of educational institution

Accrediting agencies

Law enforcement agencies

Parent of a dependent student FERPA rights holder

* + - 1. **FERPA amended by PPRA (1978) and No Child Left Behind Act (2001)**
				1. **Protection of Pupil Rights Amendment (PPRA)**: FERPA applies only to information stored in education records (directly relates to the student and is maintained by the educational institution or on behalf of the institution). PPRA provides **parents of minors** with a right to consent to, or opt out of, administration of **surveys, evaluations of analyses that collect sensitive information from students relating to any of** the following areas: political affiliation, mental and psychological problems, sex behavior and attitudes, illegal, antisocial, self-incriminating and demeaning behavior, critical appraisals of other individuals with whom respondents have close family relationships, religious practices, and income. It was a response to concerns about collection and disclosure of student information for commercial purposes – e.g., to banks and credit card companies.
				2. **No Child Left Behind Act of 2001 (NCLBA)**: No Child Left Behind amended and **broadened PPRA** to limit collection and disclosure of student survey information. Amended PPRA now **requires school to enact policies** regarding the **collection, disclosure or use of student PI for commercial purposes**, **allow parents to access and inspect surveys and other commercial instruments** before administered to students, provide **advance notice to parents** about approximate date when these activities are scheduled, and provide parents **right to opt out** of surveys or other **sharing of student information for commercial purposes**. The PPRA requirements apply to all **elementary and secondary schools that receive federal funding**. It does **NOT** apply to post-secondary schools.
			2. **FERPA and HIPAA Privacy Rule**: Privacy Rule exempts schools where educational records already subject to FERPA. **Health records of students held by school are subject to FERPA and not HIPAA**, for example, immunization records or if public elementary or secondary school provides nurse for health issues. FERPA does not apply to private elementary or secondary schools that don’t receive federal funding, so if the school qualifies as a “covered entity,” health records are subject to HIPAA Privacy Rule. At **postsecondary level**, health **records at healthcare clinic that treats only students are subject to FERPA**. FERPA and HIPAA apply ***if the clinic treats both students and non-students (e.g., faculty and staff) – FERPA applies to student health records and HIPAA Privacy Rule applies to nonstudent health records***.
		1. **Education technology**: details of students’ activities can be collected when they use educational software
			1. **Self-regulation** has become a prominent source of privacy rules applied in the educational technology space
			2. **K-12 School Service Provider Pledge to Safeguard Student Privacy** involves a dozen specific provisions, including a **prohibition on selling student PI** and a ban on **using information collected in schools for behavioral targeting of advertisements to students** – violation of the pledge makes company subject to enforcement as deceptive trade practice under Section 5 of FTC Act
			3. Main focus by state legislatures has been issues related to K–12 students – going forward, there could be increased attention on postsecondary education institutions
			4. **Ways in which privacy rules in education have evolved with technology and USG response**:
				1. The Department of Education provided guidelines on how to apply FERPA in the online arena
				2. Companies began to apply self-regulation policies which pledged to safeguard student information
				3. Violations of pledges would be subject to enforcement under Sec. 5 of the FTC
	1. **TELECOMMUNICATIONS AND MARKETING (5-7 QUESTIONS)**

**Traditional privacy tort action**: “**intrusion on seclusion**” imposes liability on one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns. Plaintiff must show that the intrusion would be highly offensive to a reasonable person

Telemarketing regulations address milder intrusions and don’t have a “highly offensive” standard.

If the **purpose of the call is a sale**, the following Rules/Acts apply.

**Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFPA)**: Requires the FTC to promulgate regulations: **(a)** defining and prohibiting deceptive telemarketing acts or practices; **(b)** prohibiting telemarketers from engaging in a pattern of unsolicited telephone calls that a reasonable consumer would consider coercive or an invasion of privacy; **(c)** restricting the hours of the day and night when unsolicited telephone calls may be made to consumers; and **(d)** requiring disclosure of the nature of the call at the start of an unsolicited call made to sell goods or services.

1. **Telephone Consumer Protection Act of 1991 (TCPA)**: FCC issued regulations under TCPA that restricts **unsolicited advertising** by phone and facsimile and **updated them in 2012 to address *robocalls*** (pre-recorded calls) and the use of automatic telephone dialing systems (***auto-dialers***) **to reconcile its rules with the TSR**. FCC has determined that these **prohibitions encompass *text messages***.
2. **Telemarketing Sales Rule (TSR)**: FTC first issued the TSR in 1995 to implement the TCFPA. Last amended in 2015. TSR 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 involves more than one interstate telephone call.” No state preemption.
	1. **Scope**: all businesses or individuals that engage in telemarketing must comply with the TSR (or the FCC counterpart) as well as applicable state laws – applies to both “**telemarketers**” (entities that initiate or receive telephone calls to or from consumers) and “**sellers**” (entities that provide or arrange to provide goods and services being offered).
	2. **Requirements for covered organizations**
		1. Call only between 8 a.m. and 9 p.m.
		2. Screen and scrub names against the national DNC list
		3. Display caller ID information
		4. Identify themselves and what they are selling
		5. Disclose all material information and terms
		6. Comply with special rules for prizes and promotions
		7. Respect requests to call back
		8. Retain records for at least 24 hours
		9. Comply with special rules for automated dialers
	3. **Entity-Specific Suppression Lists**: TSR prohibits seller (or telemarketer calling on seller’s behalf) from calling consumer asked not to be called again. Sellers and telemarketers required to maintain internal suppression lists to respect DNC requests.
	4. **Required Disclosures**: at the start of the call, before any **intended** sales content, must truthfully disclose (telemarketing call cannot be called a “courtesy call”):
		1. identity of seller
		2. that purpose of call is to sell goods or services
		3. nature of those goods or services
		4. for prize promotion: no purchase or payment necessary to participate or win, and purchase or payment does not increase chances of winning
	5. **Misrepresentations & Material Omissions**: prohibited during sales calls. Requires telemarketers to meet a higher standard for proving authorization when consumers use new payment methods since many new methods lack protections of credit cards.
	6. **10 categories must always be disclosed**:
		1. Cost and quantity
		2. Material restrictions, limitations or conditions
		3. Performance, efficacy or central characteristics
		4. Refund, repurchase or cancellation policies
		5. Material aspects of prize promotions
		6. Material aspect of investment opportunities
		7. Affiliations, endorsements or sponsorships
		8. Credit card loss protection
		9. Negative option features
		10. Debt relief services
	7. **Transmission of Caller ID Information**: requires telemarketing calls to transmit accurate call identification information (name and phone #) for telemarketer or seller on whose behalf the call is made so that it can be presented to consumers with caller ID services. Seller’s customer service number may be used if answered during normal business hours. Telemarketer not liable for isolated, inadvertent instances when Caller ID information fails to make it to consumer’s receiver.
	8. **Call Abandonment Prohibited**: expressly prohibits telemarketers from abandoning an outbound telephone call with either “hang-ups” or “dead air.” Outbound call is “abandoned” if person answers and the telemarketer does not connect call to live sales rep within 2 seconds of person’s completed greeting.
		1. **Violations of TSR:** Abandoned calls resulting from telemarketer’s use of predictive dialers to simultaneously call multiple consumers at the same time and use of prerecorded-messages that deliver sales pitch - **prerecorded sales messages must have prior express consent (opt-in) of consumer**.
		2. **Abandoned Call Safe Harbor**: telemarketer will not face enforcement action for violating call abandonment prohibition if telemarketer ensures live rep takes at least 97 percent of calls answered by consumers (i.e., calls answered by machine, not answered at all, or made to nonworking numbers do not count). Safe harbor **applies if Telemarketer**:
			* Uses technology to ensure **abandonment of** **no more than 3%** **of all calls answered by live person** (per day per calling campaign over 30-day period)
			* Allows phone to **ring for** **15 seconds or 4 rings** before disconnecting unanswered call
			* Plays **recorded message** stating **name and phone number of seller** when live sales rep unavailable within 2 seconds of live person answering call
			* Maintains **records documenting compliance** withpreceding 3 requirements
	9. **Prohibition on Unauthorized Billing**: prohibits telemarketers from billing consumers for any goods or services without the consumer’s “express, informed consent.” Providing billing account info during the call amounts to non-deceptive express, informed consent.
		1. **Special Rules for Free Trials** (fee-to-pay conversions) to combat unauthorized charges at end of free trial. Telemarketer must:
			* Obtain from customer **at least last 4 digits of account #** to be charged
			* Obtain customer’s **express consent** to be charged for goods or services using that account number
			* Make and maintain **audio recording** of entire telemarketing transaction
	10. **FCC Updates on TCPA re Robocalls & Auto-dialers to mirror TSR**
		1. **No existing business relationship (EBR) exemption for robocalls** – prior express ***written*** ***consent*** required for robocalls to ***residential lines***
		2. Required to provide consumers opportunity to **opt-out of future robocalls during a robocall**
		3. Robocalls made by **entities subject to** **HIPAA are exempt** from above requirements
		4. These revisions increased harmonization with FTC rules on abandonment
	11. **Updates on FCC Approach to Robotexts**
		1. 2015 TCPA prohibits robotexts (i.e., sending messages w/o human intervention) without **express written consent** that includes “**clear and conspicuous disclosure**” that telemarketing calls or texts can be made with an **autodialer or artificial voice** and was **not obtained as a requirement of purchase**.
		2. 2017 additional robotext guidance
			* **consent can be revoked** by consumer at any time by any reasonable means
			* fact that consumer’s wireless number appears in **contact list of another** wireless customer **insufficient to establish consent**
			* when caller has consent for wireless number and **number reassigned**, caller **not liable for first call** but will liable for subsequent calls if new consumer makes caller aware of change
	12. **Recording-Keeping Requirements**: TSR requires sellers/telemarketers to keep **substantial records** for **2 years** from date record is produced
		1. Advertising and promotional materials
		2. Information about prize recipients
		3. Sales records, which **must include**
			* Name and last known home address of each customer
			* Goods or services to be purchased
			* Date goods or services were shipped/provided
			* Amount customer paid for goods/services
		4. Employee records, which **must include** for all **current and former** employees **directly involved in phone sales**
			* Name
			* Last known home address and phone number
			* Job title
			* All verifiable authorizations or records of express informed consent or express agreement
	13. **Enforcement**
		1. FTC, State AGs, or private individuals
		2. **Penalties**:
			* TSR violations - civil penalties up to $42,530/call
			* May have private right to action for tort of intrusion on seclusion
	14. **TSR National Do-Not-Call registry (DNC)**: provides means for U.S. residents to register **residential and wireless** phone numbers on which do not wish to be called **for telemarketing** purposes.
		1. **Scope**: applies to **for-profit organizations**, **including** **charitable solicitations placed by for-profit** **telefunders** (i.e., telephone fundraising by for-profit telemarketers who call potential donors seeking donations on behalf of charities)
		2. **Enforcement**: FTC, FCC and State AGs
		3. **Penalties**: civil penalties of up to $42,530 per violation and violators may be subject to nationwide injunctions prohibiting certain conduct and monetary damages to injured consumers
		4. **Compliance**: sellers/telemarketers **must access registry** **before** making any solicitation calls
			* Violation of TSR to call consumer unless registry is checked, **even if consumer’s name and number not on list**
			* Only **sellers**, **telemarketers**, and **their service providers** **can access DNC registry** using unique Subscription Account Number (**SAN**), which is **not transferable**
			* Fees to access registry are based on area codes requested and paid for by holder of the SAN
				+ Telemarketer accessing registry **on behalf of seller-clients** are required to identify and provide **seller-client’s unique SAN**
				+ Telemarketer accessing **on its own behalf** needs its **own unique SAN**
			* **Requirements of sellers / telemarketers**
				+ Update their call lists every **31 days** with new registry information
				+ Screen and scrub names against national DNC list
		5. **Exceptions to the DNC Rules**: DNC rules do not apply to
			* **Nonprofit** calling **on its own behalf**
			* Calls to **customers with existing business relationship** (**EBR**)
				+ If consumer has not requested to be on entity-specific DNC list
				+ EBR “**customer**” if purchased, rented or leased goods/services or otherwise completed transaction (date of last payment, transaction or shipment) with seller in ***last 18 months***
				+ EBR “**prospect**” if made **application or inquiry** regarding goods/services w/in ***last 3 months***
				+ Inbound calls if **no “upsell” of additional** products or services
			* Most **B2B** calls
			* **Consent**: sellers/telemarketers can call consumers who consent **to receive calls**
				+ Seller’s **request for consent** must be “**clear and conspicuous**” and no subterfuge

**If in writing**, cannot be: hidden; printed in small, pale or non-contrasting type; hidden on back or bottom of document; or buried in unrelated information

**If online**, the “please call me” button cannot be pre-checked

* + - * + **Consent** must be **in writing**, must **state the number** to which calls may be made, and must include **consumer’s signature** (including valid e-signature)
		1. **DNC Safe Harbor**: Seller/telemarketer not subject to civil penalties or sanctions for **erroneous call** to consumer who asked not to be called or is on DNC list **if, as part of routine business practices**:
			- established and implemented written procedures to honor consumers’ requests that they not be called, **[and]**
			- trained its personnel, and any entity assisting in its compliance, in these procedures, **[and]**
			- has, or someone else acting on behalf of seller has, maintained and recorded an entity-specific DNC list, **[and]**
			- uses (and maintains records documenting) process to prevent calls to number on entity-specific DNC list or National DNC registry if the latter involves using version of National Registry from FTC no more than 31 days before date any call made, **[and]**
			- monitors and enforces, or someone else acting on behalf of monitors and enforces, compliance with entity’s written DNC procedures.
	1. **State Telemarketing Laws**: majority of states have enacted telemarketing laws
		1. >50% of states require telemarketers to obtain license or register with the state
		2. States can have **their own DNC lists** with **different exceptions, fines** or consumer **enrollment methods**
		3. Some states require **telemarketers to ID themselves** at start of call or **terminate call w/o rebuttal** if consumer so desires
		4. State may require **written contract for certain transactions**
1. **The Junk Fax Prevention Act of 2005 (JFPA)**: **No unsolicited fax advertisements**
	1. No exception for accidental transmissions
	2. Fines of $500 / page for violations
	3. Fines of $1500 / page for knowing or willful violations
	4. Consent required for unsolicited commercial fax transmissions
	5. **Exception to TCPA - Consent is implied from an Existing Business Relationship (EBR)**.
		1. **EBR Consent Requirements**:
			* **Voluntary** provision of fax number to sender
			* **1st page of fax must include**
				+ **instructions for opting out** from future faxes, including at least 1 free mechanism for opting out that must be available 24/7
				+ **contact info for sender**, including US phone and fax numbers
				+ the **notice** must be **clear and conspicuous**
	6. EBR has same definition as FTC’s DNC rule
2. **Combating the Assault of Non-solicited Pornography and Marketing Act of 2003 (CAN-SPAM)**: **Preempts most state laws** that restrict commercial email communications, **but** CAN-SPAM does **not** supersede **state** **spam laws to the extent** the laws **prohibit false or deceptive activity**
	1. **Scope**: covers **transmission** directed to or originating from US of **unsolicited** **commercial e-mail messages** whose primary purpose is advertising or promoting product or service – not intended to stop commercial email but to provide mechanism for legitimate prospecting while respecting individual right to opt-out of unwanted communications
		1. **Three Categories of Email**
			* **Commercial**: messages that advertise or promote commercial product/service
			* **Transactional/Relationship**: messages that facilitate or confirm a transaction the recipient has already agreed to
				+ Facilitate or confirm a transaction
				+ Provide warranty, recall, safety or security information
				+ Give info about changes in terms of existing account
				+ Provide info about employment relationship
				+ Deliver goods/services
			* **Other**: messages that are not commercial, transactional or contain relationship content
	2. **Requirements**
		1. **No false or misleading headers**
		2. **No deceptive subject lines**
		3. Commercial emails must contain functioning, clearly and conspicuously displayed **return email address** that allows recipient **to contact sender**
		4. Commercial email must contain clear and conspicuous notice of **opportunity to opt out/unsubscribe at no charge**, such as by return email or an opt out link
		5. **Honor individual request not to receive future email** by not sending commercial email (following a grace period of 10 business days)
		6. **All commercial email must include**:
			* Clear and conspicuous **identification as commercial message** (unless prior affirmative consent) and
			* A **valid physical address of sender**
		7. **No aggravated violations** relating to commercial email, such as
			* **Address-harvesting and dictionary attacks**
				+ **Address-harvesting** means obtaining the address using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages
				+ **Dictionary attack** means obtaining the address of the recipient using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations
			* **Automated creation of multiple email accounts**
			* **Retransmission** of commercial email **through unauthorized accounts**
		8. All email containing **sexually oriented material** must include **warning label** (unless recipient gave prior affirmative consent to receive the email) – **CAN-SPAM Adult Labeling Rule** requires phrase “SEXUALLY-EXPLICIT:” to appear in all caps as first 19 characters in subject line
	3. **Does not apply to “transactional or relationship messages” where primary purpose is to**:
		1. Facilitate or confirm agreed-upon commercial transaction
		2. Provide warranty or safety information about product purchased or used by recipient
		3. Provide information regarding ongoing commercial relationship
		4. Provide information related to employment or related benefit plan
		5. Deliver goods or services to which recipient entitled under terms of agreed transaction
	4. **Enforcement**: FTC, other federal regulators, State AGs and other state officials. **ISPs can sue violators for injunctive relief and monetary damages – no private right of action for anyone else**
	5. **Penalties**: fines up to $42,530 per violation (i.e., each separately addressed unlawful commercial message); for those authorized to sue, injunctive relief and damages up to $250/violation with max of $2M. Court may increase damage award up to 3X amount otherwise available in cases of willful or aggravated violations. Certain egregious conduct punishable by up to 5 years imprisonment.
	6. **Wireless Message Rules Under CAN-SPAM**: FCC rules implementing CAN-SPAM with regard to mobile service commercial messages (MSCMs), including many commercial text messages. MSCM defined as “commercial email message transmitted directly to wireless device used by subscriber of commercial mobile service.” **Message must have (or use) unique email address that includes “a reference to an Internet domain.”** Messages not sent to an address for a wireless device but forwarded to wireless device are not subject to FCC rules on MSCMs. FCC’s rules cover messages sent using SMS (texting) technology but not phone-to-phone messages. FCC defers to FTC rules and interpretation regarding definitions of “commercial” and “transactional” with respect to email messages as well as mechanisms for determining “primary purpose” of a message. FCC rule must be analyzed in context of FTC regulatory framework for CAN-SPAM.
		1. **MSCM text messages = SMS** (short message service) and **MMS** (multimedia message service)
		2. If destination is email address (@ plus domain name) => CAN-SPAM and FCC wireless email rules
		3. If destination is phone number => TCFPA, TCPA (FCC) and TSR (FTC)
	7. **Express Prior Authorization**: **CAN-SPAM** prohibits senders from sending mobile service commercial messages (MSCMs) without subscriber’s “express prior authorization.” Express prior authorization must be obtained for each MSCM, regardless of sender or industry. **FCC requirements**: Express authorization means opt-in - affirmative action to give authorization – not a negative option or omission of action (e.g., opt out). Sender can’t send MSCMs on behalf of 3rd party (including affiliates and marketing partners). Revocation must be enabled by same means used to grant authorization. FCC rule **maintains** that CAN-SPAM **10 business day grace period following revocation**. FCC requires that **authorization must includ**e:
		1. subscriber agreeing to receive MSCMs sent to wireless device from a particular (identified) sender
		2. subscriber may be charged by their wireless provider in connection with receipt of messages
		3. subscriber may revoke authorization at any time
	8. **The Wireless Domain Registry**: to help senders of commercial messages determine whether messages might be mobile service commercial messages (MSCMs) rather than commercial email, FCC created registry of wireless domain names (available on FCC website). Senders are responsible for obtaining the list and ensuring appropriate authorizations exist before sending commercial messages to addresses within the domains, so requirements listed above apply to messages sent to any address whose domain name is included on wireless domain name list.
3. **Telecommunications Act of 1996**: **Section 222** of the act governs the privacy of customer information provided to and obtained by telecommunications carriers (including ISPs) and VoIP providers.
	1. Imposed new restrictions on access, use and disclosure of **customer proprietary network information (CPNI)**
		1. **CPNI is data collected by telecommunications carriers about their subscribers phone calls**. Includes info typically included in your phone bill, such as subscription info, services used, and network and billing info, call log data (calls dialed), such as time, date, destination & duration of calls. *Personal info such as name, telephone number, and address are* ***not*** *CPNI.*
		2. Carriers can use and disclose CPNI **only w/customer approval** or as required by law. Carriers do NOT need approval to use, disclose, or provide marketing offerings among service categories that customers already subscribe to. CPNI can also be used for billing and collections, fraud prevention, customer service and emergency services.
		3. Carrier can use **CPNI** for **its own purposes** unless consumers **opt out**
		4. Customers must expressly consent, or **opt in,** **before carriers can share their CPNI** w/joint venture partners and independent contractors **for marketing purposes**.
		5. **Carriers must notify law enforcement when CPNI is disclosed in a security breach** **w/in 7 business days** of that breach, also **customers must provide a password** **to access their CPNI** via phone or online account services.
		6. Carriers must **certify 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**.
	2. Privacy of customer information provided to and obtained by telecommunication carriers
	3. Limits use, access, and disclosure of CPNI
	4. **Enforced by FCC**.
4. **Cable Communications Policy Act of 1984** (Cable Act): promotes competition and deregulated cable TV industry
	1. Cable service provider **prohibited** from
		1. **collecting PII w/o written or electronic consent** unless necessary to
			* provide cable service
			* detect unauthorized reception of service
		2. **disclosing PII** unless
			* **required to provide service** or conduct other legitimate business activities
			* subject to **court order** and provider **notifies subscriber** when receives court order
				+ Electronic Communications Privacy Act (ECPA) of 1986 allows these disclosures w/o notice to consumer, since notice might impact ongoing investigation
				+ Courts have resolved conflict in favor of ECPA due to its enactment after Cable Act
			* **limited to name and address** of subscriber IF subscriber given **option to opt out** or **limit disclosure** and **no information provided about services or viewing habits** of subscriber
	2. **Requires cable service providers** to provide subscribers **initially and annually** thereafter **privacy notice** that **clearly and conspicuously informs them of**
		1. nature of PI collected
		2. nature, frequency, and purpose of any possible disclosures of that information
		3. rights of subscribers to enforce limitations on collection and disclosure of information
		4. how to access or correct
		5. No specified schedule for **data retention/destruction**, but mandates that PI must be destroyed when no longer needed for the purpose for which collected and no pending requests for access
	3. **Enforcement**: Enforced by FCC. Provides a **private right of action** for the above and allows for **actual or statutory damages, punitive damages and reasonable attorney’s fees and court costs**
	4. **Does not regulate provision of broadband Internet services** **via cable** because Act defines “cable service” as one way transmission to subscribers of video
5. **Video Privacy Protection Act of 1988 (VPPA)**: passed in response to disclosure and publication of then-Supreme Court nominee Robert Bork’s video rental records, which was thought to be gross violation of privacy
6. **Scope**: applies to “**video tape service providers (VTSP)**,” who are defined as anyone “engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials” **AND** individuals who **receive PI in the ordinary course** of a VTSP’s business OR for **marketing** purposes
	* + 1. Prohibits the *knowing* disclosure by VTSP of **information identifying a person as having requested or obtained specific video materials or services** from the VTSP
			2. **Online streaming services and online video content providers are VTSPs** and subject to the VPPA – dated language in the VPPA creates uncertainty and expensive class action litigation
7. **VTSP prohibited from disclosing consumer’s** (renter, purchaser or subscriber) **PI** **unless** disclosure is made according to one of the following **exceptions**:
	* + 1. to the consumer themselves
			2. subject to **contemporaneous written consent** of consumer
			3. to **law enforcement** pursuant to a **warrant, subpoena or other court order**
			4. includes **only names and addresses** of consumers
			5. includes **only** **names, addresses *and subject matter descriptions*** **IF** the disclosure **used by 3rd party only** **for marketing goods or services to the consumer** (e.g., VTSP can disclose customer list to 3rd party and, in the process, disclose data not otherwise permitted to be disclosed (i.e., subject matter description of video content consumption), for sole purpose of direct marketing)
			6. for order fulfillment, request processing, transfer of ownership, or debt collection
			7. pursuant to a **court order in a civil proceeding and consumer granted right to object**

The permitted disclosures help avoid liability for disclosures by VTSPs whose business name is enough to create an inadvertent prohibited disclosure (e.g., specialty VTSP with limited subject matter), and the ‘exception to the exception’ (#5 above) assists a business wanting to disclose an individual’s content viewing to facilitate the sending of direct marketing to that consumer – but they don’t solve problems created by modern social media sharing of video content consumption.

1. Requires **PI to be destroyed** “as soon as practicable, but **no later than 1 yr from date no longer necessary** for the purpose for which collected **and** **no pending requests** or orders **for access**
2. Allows **private right of action** for disclosure-related violations (not based merely on improper retention of PI) and allows for

1. actual or statutory ($2500) damages

2. punitive damages and

3. reasonable attorney’s fees and court costs

1. **Does not preempt stricter state law**
2. **Video Privacy Protection Act Amendments Act of 2012 (H.R. 6671)**: sought to address integration of video content consumption by users with 3rd party social media platforms (e.g., Netflix users sharing movie viewing info on FB) b/c VPPA provided VTSPs no mechanism or exception to permit such ‘social sharing’ or data exchange
	* + 1. **Disclosure to 3rd parties** of **video content consumption** permitted **if consumer gives** ‘**informed, written consent** (including through an electronic means using the internet)… in a form **distinct and separate from** any form setting forth other legal or financial obligations of the consumer… **at the time** the disclosure is sought, **or in advance** for a set period of time’ (**up to two years**). The user has to be given **clear and conspicuous opportunity to withdraw** (opt-out) on a case-by-case basis or from ongoing disclosures
			2. Allows one-time **consumer consent valid for up to 2 years**, replacing the contemporaneity requirement
			3. Several states including CA have enacted laws covering privacy issues similar to VPPA
3. **Recent Developments**
	* + 1. consumers who use free mobile applications do not qualify as ‘subscribers’ under the VPPA
			2. intra-corporate disclosure of personal information does not violate the VPPA
			3. VTSPs not liable under VPPA for circumstances where subscribers’ personal information was displayed on devices, such as televisions, that could potentially be viewed by 3rd parties, because viewing of such devices beyond VTSP’s control
			4. **applicable PII for purposes of VPPA ‘is information which must, without more, itself link an actual person to actual video materials’**
			5. **3rd Circuit Court of Appeals in Plaintiff v Viacom & Google** (Nickelodeon privacy litigation): VPPA only allows consumer to sue a person or entity that discloses ‘personally identifying information,’ and not a person who **merely receives** such information; and PII under VPPA ‘applies only to the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior.’
* IP addresses, device identifiers, or browser fingerprints do not meet this requirement and therefore fall outside of the scope of the VPPA
* However, court said its interpretation subject to state of the art - digital identifier may be sufficient to impose liability under VPPA in the future
	+ - 1. **No comparable legislation in EU** – any processing or disclosure of such “personal data” would be permitted with appropriate notice and consent mechanisms.
1. **Digital Advertising**: desktop/laptop and mobile advertising as an integral part of marketing, with mobile advertising accounting for more than two-thirds of digital advertising spending
	1. **Self-Regulation for Online Advertising**: privacy concerns raised by the tracking associated with digital advertising have led companies involved in desktop/laptop advertising and mobile advertising to **voluntarily bind themselves to self-regulatory principles**
		1. **Digital Advertising Alliance (DAA)** Self-Regulatory Principles for Online Behavioral Advertising: **nonprofit** organization that collaborates with businesses, public policy groups and public officials to **establish and enforce** “**responsible privacy practices** across industry for relevant digital advertising, **providing consumers with enhanced transparency and control**.” Principles include:
			* **guidelines** for interest-based advertising in desktop/laptop and mobile environments and for cross-device use of data
			* **consumer management of opt-outs**
			* **Oversight and Enforcement** - Better Business Bureau and Direct Marketing Association
		2. **Network Advertising Initiative (NAI) Code of Conduct**: **nonprofit** self-regulatory association of third-party digital advertising companies. The NAI Code is a list of self-regulatory principles that all NAI members agree to uphold, including:
			* **Notice and choice** for interest-based advertising
			* **Limits on the types of data that that can be used** for advertising purposes
			* Substantive **restrictions on collection, use, and transfer of data** used for online behavioral advertising
			* **Enforcement** - **its board**, w/sanctions including revocation of membership and **referral to FTC**
		3. **Violations by members of DAA and NAI** are considered **“unfair and deceptive” practices** that can lead to **FTC and State AG general enforcement** actions
	2. **Federal Regulation: FCC Broadband Privacy Rule**: Nullified as of April 4, 2017 by Trump
		1. 2015: FCC reclassified broadband internet service as a public utility as part of its “Open Internet” or net neutrality rule.
		2. June 2016: US Ct of Appeals upheld FCC’s authority to regulate broadband internet providers, which included traditional phone providers and cable companies
		3. Effect of reclassification was broadband internet service providers subject to requirements of Telecom Act of 1996, including CPNI privacy requirements of Section 222
		4. Nov 2016: FCC adopted broadband privacy rules that
			* required customer opt-in for uses of sensitive personal information
			* allowed use of customer opt-out for uses not involving sensitive personal information
			* permitted inferred customer consent for providing underlying services and related uses
			* provided guidelines for data security and breach notification
		5. April 2017: Congress votes under Congressional Review Act to rescind FCC broadband privacy rule and Trump signed the law that cancelled the rule, **BUT** reclassification of **broadband internet service providers as public utilities remained intact**.
		6. FCC issued order stating that Section 222 and CPNI rules apply to broadband internet service providers under general provisions of Section 222 instead of the stricter 2016 rules
	3. **State Regulation: California Online Privacy Protection Act 2003 (CalOPPA)**: 1st US law to require operators of commercial websites and online services, including mobile apps, to **“conspicuously post” privacy policy if collect PII from CA residents** (e.g., icon or text link including word “privacy” linked to privacy policy or text link in capital letters at least same size as surrounding text, or larger text, contrasting type, font or color or otherwise written in way that calls attention to the link, such as set off by symbols or other marks).
		1. **Do Not Track (DNT) Technology** enables consumers to communicate desire not to be tracked through browser
		2. **2013**: amended to address issues of **online tracking -** collection of personal information about consumers as they move across web sites and online services. Requires web site operators and online services to ***inform consumers how sites and services respond to DNT signals from browsers***.
		3. **Privacy policies must disclose** (no requirement to elaborate):
			* **Categories of PII** collected through the site (no specificity required about PII, how it’s collected, whether cookies or web beacons are used or retention period)
			* **Categories of 3rd parties** with whom site operator can share PII or other content (no need to identify affiliates or marketing partners or provide links to 3rd party privacy policies)
			* **Do Not Track Disclosure**: How site operator responds to web browsers’ **Do Not Track** **signals** or other mechanisms that provide consumers the ability to choose regarding collection of PII about consumer’s online activities over time and across 3rd party websites (there’s no requirement that the website actually respond to the DNT signal)
				+ CalOPPA only requires that tracking disclosures be included **somewhere in the privacy policy**
				+ website operator can comply by providing a **“clear and conspicuous hyperlink” in its privacy policy** to an online location containing a description and the effects of a program or protocol that site operator follows to offer users a choice regarding online tracking (CA AG guidance states this is more transparent than a link to a “choice program”)
			* **3rd Party Tracking**: Whether 3rd parties **are or may be** collecting PII and conducting tracking while consumer is on the operator’s site or service
		4. **Privacy Policy Does Not Need to Explain**:
			* How site uses PI beyond what’s necessary to fulfill transaction or provide online service
			* With which 3rd parties it shares PI
			* Consumer choices regarding collection, use or sharing of PI other than review and correction of PI
			* Site’s security safeguards or provide contact for questions
2. **GOVERNMENT AND COURT ACCESS TO PRIVATE-SECTOR INFORMATION (6-8 QUESTIONS)**
	1. **LAW ENFORCEMENT AND PRIVACY (3-5 QUESTIONS)**

Along with civil litigation, a company can face requests to provide personal information in connection with criminal investigations and litigation. **Fourth Amendment limits on law enforcement searches – “reasonable expectation of privacy test” developed in context of government wiretaps**. Statutes that can apply to criminal investigations, including HIPAA, ECPA, SCA, RFPA. **CLOUD Act addresses evidence stored in other countries**.

* + 1. **Fourth Amendment**: ***The 4th Amdt articulates many of the fundamental concepts used by privacy professionals in the U.S.*** SCOTUS stated that “the overriding function of the 4th Amdt to protect personal privacy and dignity against unwarranted intrusion by the State.” Evidence obtained in violation of the 4th Amdt is subject to the “exclusionary rule” – the evidence can be excluded from a criminal trial.

***Olmstead v. US (1928)***: SCOTUS held no warrant was required for wiretaps conducted on telephone company wires outside of the suspect’s building. 4th Amdt only protects home and other private spaces

***Katz v. US (1967)***: SCOTUS overruled Olmstead and held that **warrantless wiretaps are unconstitutional searches**, because there was a **reasonable expectation that communication would be private**. Reasonable expectation of privacy test. What a person knowingly exposes to the public, even in his own home or office, is not protected by 4th Amendment. [J. Brandeis] “There is a twofold requirement, first that a person have exhibited an **actual (subjective) expectation of privacy** and, second, the **expectation is one that** **society** **recognizes as ‘reasonable**.’”[J. Marshall] **[*In Public Exception*]**

***US v Miller (1976)***: SCOTUS held that the 4th Amdt does not require a warrant for police to get a person’s checking account records or the list of phone numbers a person has called. **Information a person puts into hands of a 3rd party not protected by 4th Amdt**. **[*Third Party Doctrine*]** Companies are permitted to turn over customer and employee records to the government (although statutory and other legal limits may apply).

***US v Jones (2012)***: Held that a warrant was needed when the police placed a GPS device on a car and tracked its location for over a month. Decision emphasized that the police had **trespassed onto car when physically attached GPS device**. Concurring opinions implied Constitutional limit on surveillance of “in public” activities, potential implications for 3rd party doctrine.

***Riley v California (2014)***: SCOTUS held that the **contents of cell phone cannot be searched by law enforcement w/o a search warrant**. Data on cell phone was quantitatively and qualitatively different than information in a physical container. Immense storage capacity of cell phones as well as ability to link to remote storage. Internet searches can reveal a person’s interests, and location information can pinpoint individual’s movement over time.

***Carpenter v US (2018)***: SCOTUS held that law enforcement officers must secure a warrant to access at least certain records held by third parties namely, cell site location information.

Recent cases suggest SCOTUS seeking to update 4th Amdt doctrine to adapt to changing technology and may place further limits on 3rd party doctrine as it relates to digital data.

1. **Access to Financial Data**: Disclosure to law enforcement prohibited unless statutory requirements met
	* + 1. **Right to Financial Privacy Act of 1978 (RFPA)**: passed after the Supreme Court held in *Miller* that 4th Amdt did not apply to checking accounts
				1. Applies to **disclosures by** **financial institutions**: banks, credit card companies and consumer finance companies **requested by federal agencies**
				2. For **financial records of individuals** and **partnerships of fewer than 5 people**.
				3. No government authority can access or obtain copies of information contained in financial records of any consumer from a FI unless **financial records are reasonably described** ***and*** meet **one of the following** conditions:

**customer authorization**

**administrative subpoena or summons** (e.g., by a federal agency)

**qualified search warrant** (a showing of probable cause, specifying person to be seized, place to be searched and evidence being sought and signed by a neutral magistrate)

**judicial subpoena or summons**

**formal written request from authorized gov authority for law enforcement**

* + - * 1. **Notice**: Agency must provide customer with written notice of government request for records and wait 10 days from service or 14 days from mailing to access the records. **Customer has right to object to the disclosure in court**.
				2. **Penalties**: actual damages to the customer, punitive damages, and attorney’s fees
			1. **Bank Secrecy Act of 1970 (BSA)**: “**The Currency and Foreign Transaction Reporting Act**”
				1. **Basis of the law**: Targeted organized crime groups and others who used **large cash transactions**
				2. **What it does**: Authorizes **Treasury Secretary** to issue regulations that impose **extensive record-keeping and reporting requirements on FIs**
				3. **Applies to** any entities subject to supervision by state or federal bank supervisory authority (banks, securities brokers, casinos, card clubs, etc.)
				4. **Requirements**: FI must keep records and file reports on **certain financial transactions**:

**Currency Transaction Reports (CTR) –** institution must report cash transactions totaling **more than** **$10,000** in a single day

Exception: does not include **credit secured by real property**

**Suspicious Activity Report (SAR)** – institution must report **suspected money laundering** activity ***or*** **attempts to deliberately avoid CTRs**. (see below for more)

**bank checks, drafts, cashier’s checks, money orders, or travelers’ checks for $3000 or more in currency**

Must collect **name, address and SSN** of the purchaser; **date** of purchase; type of **instrument**, and **serial numbers and dollar amounts** of the instruments

**Exceptions** to records and reports requirements:

Funds governed by the **Electronic Funds Transfer Act** and

Transactions made through **automated clearinghouses, ATMs or point of sale systems**

* + - * 1. **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 **5 years**

For deposit account records:

Depositor’s taxpayer ID

Signature cards

**Checks exceeding $100**

* + - * 1. **Suspicious Activity Reports (SAR)**

FI must file in certain situations. Alerts government to suspicious transactions

Must be filed with the U.S Department of Treasury’s Financial Crimes Enforcement Network (Fincen) when:

FI **suspects** an **insider committing crime** regardless of dollar amount

entity **detects** **crime involving $5000** and **substantial basis for identifying suspect**

entity **detects** **crime involving $25,000** (no need for suspect)

entity **detects currency transactions aggregating $5000 or more** that involve **potential money laundering**

* + - * 1. **Violations**

**Civil Penalties** including

fines up $25000 or the amount of the transaction (up to $100,000 max)

penalties for negligence ($500/violation).

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 $1M for failure to comply with due diligence requirements

**Fines** for negligence, failure to comply with regulations, failure to comply with information sharing requirements, 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.

1. **Access to Communications**: From strictest to most permissive, federal law has **different rules for** (1) telephone monitoring and other tracking of **oral communications**, (2) privacy of **electronic communications**, and (3) **video surveillance**, for which there is little applicable law. Federal law is also generally **stricter for real-time interception** of a communication **than retrieval of a stored record**. In each area, states may have statutes that apply stricter rules. Potential state law claims for invasion of privacy or other common-law claims when monitoring is offensive to a reasonable person.
2. **Wiretaps**: federal law generally **strict in prohibiting wiretaps of phone calls – requires probable cause and search warrant plus alternative means of getting the evidence have been exhausted**. **Exceptions**: Interception is permitted if the party to the call or if **one of the parties** has given **consent** and where companies **intercept in the ordinary course of business**
3. **Electronic Communications Privacy Act (ECPA)**: passed after SCOTUS held that 4th Amdt did not apply to phone numbers called. Protects **wire, oral, and electronic communications** **while** those communications are **made, in transit, and stored** on computers. The Act applies to **email, telephone conversations, and data stored electronically**. ECPA included amendments to the Wiretap Act (Omnibus Crime Control and Safe Streets Act), created the Stored Communications Act, and created the Pen Register Act. **ECPA prohibits US service providers from disclosing content of communications to law enforcement except through a warrant or an appropriate request through another mechanism**.
	* + 1. **Wiretap Act**: concerns **interception of electronic and wire communications**, which include “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection” – **any oral conversation where person has no expectation that 3rd party is listening**. **Covers communications while made/in transit**.

**Prohibitions**:

wiretapping and electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and use or disclosure of information unlawfully obtained through wiretapping or electronic eavesdropping

**intentionally intercepting or attempting to intercept a wire, oral or electronic communication** by **using any electronic, mechanical or other device** - electronic device must be used to perform surveillance; **mere eavesdropping with unaided ear not illegal under ECPA**

disclosing information so obtained if person has reason to know was obtained illegally through interception of a wire, oral, or electronic communication

**Exceptions:**

interception **authorized by statute for law enforcement purposes**

**consent of at least one of the parties** is given – some states require consent of all parties

**individual record’s own conversation** without violating federal law

* + - 1. **E-mails and** **Stored records**: **Stored Communications Act (SCA)**: addresses access to **stored communications at rest**, which primarily means e-mails that are not in transit.

**Prohibits unauthorized acquisition, alteration, or blocking of electronic communications while electronically stored in a facility through which electronic communications service is provided**

Exceptions for law enforcement access and user consent

Employer cannot access employee's private e-mails unless consent is given (e.g., employment contract that explicitly authorizes employer to access e-mails)

Violations can lead to criminal penalties or a civil lawsuit

**State laws may protect emails**. **Delaware** prohibits employers from monitoring or intercepting **phone** conversation or transmission, **email** or transmission or **internet** access or usage w/o prior written notice and daily electronic notice. **Connecticut** requires employer who engages in electronic monitoring to give **prior written notice to all employees** and post **notice of types of electronic monitoring in conspicuous place**.

* + - 1. **Pen registers (communications metadata)**: **Pen Register Act** covers pen registers/trap and trace. Pen registers are **surveillance devices that capture phone numbers dialed on outgoing phone calls**; **trap and trace devices** capture numbers identifying **incoming calls.** Not supposed to reveal content of communications or identify parties to a communication or whether a call was connected - only that **one phone dialed another phone**.

**Smith v Maryland**: SCOTUS held that **a pen register is not a search because “petitioner voluntarily conveyed numerical information to phone company**.**”** Court did not distinguish between disclosing numbers to human operator or just automatic equipment used by phone company. Left pen registers completely outside constitutional protection. **No reasonable expectation of privacy in the information because telecom company has ready access to it**.

* Standard for the government to obtain a pen/trap order is much lower than that required for a wiretap – must only be “relevant to an ongoing criminal investigation”
* In context of phone calls, pen registers display outgoing number and incoming number.
* USA Patriot Act expanded beyond phone numbers to include “dialing, routing, addressing, or signaling information” transmitted to or from a device or process.
* Because e-mail subject lines contain content, pen registers in e-mails must include sender and addressee but NOT any part of subject line (per revisions in the USA Patriot Act)
* USA Freedom Act prohibits use of pen registers and trap and trace orders for bulk collection and restricts use to circumstances where there are specific selectors, such as email address or phone number
* IP addresses and port numbers associated with communication are allowed
* Prohibits installation or use of any device (including software) that serves as a pen register or trap and trace
	+ - 1. **CalECPA**: No California government entity can search phones and no police officer can search accounts without:

Permission from a **judge**

Obtaining **consent**

Showing it is an **emergency**

1. **The Communications Assistance to Law Enforcement Act of 1994 (CALEA) (Digital Telephony Bill)**:
	* 1. **Scope**: Does not add any new wiretapping authority. Requires **telecommunications carriers** to assist with implementation of authorized wiretaps. In 2005, FCC issued order that **expanded scope** of telecom services **to** **providers of broadband internet access and VOIP services when interconnect with traditional phone services**
		2. **Applies** to **phone companies** and other common carriers, **VoIP service provider**s and **internet service providers**
		3. **What it does**: lays out the duties of defined actors in the telecom industry to cooperate with intercepting communications for law enforcement, and other needs relating to security and public safety.
		4. Implemented by **FCC**
	1. **NATIONAL SECURITY AND PRIVACY (1-3 QUESTIONS)**

**When the government seeks personal information for national security purposes**. Any company can be faced with a request for records under Section 215 of the USA Patriot Act, and many can receive NSLs. Responding to national security requests is complicated because US privacy laws have varying scope and differing definitions for national security exceptions.

* + 1. **Foreign Intelligence Surveillance Act of 1978 (FISA)**: Establishes standards and procedures for the authorization of **electronic surveillance** (including video) that collects foreign intelligence, use of **pen registers and trap and trace devices** (for phone numbers, email addresses, and other addressing and routing information), **physical searches**, and **business records** for the purpose of gathering foreign intelligence within the US. FISA orders can be issued when **foreign intelligence gathering** is **significant purpose** of investigation. FISA orders are issued based on **probable cause that** **party to be monitored** (any person – even US person) is “**foreign power**” or “**agent of a foreign power**.” FISA orders issue from a **special court of 11 federal district court judges**, the **Foreign Intelligence Surveillance Court (FISC)** – holds secret hearings on FISA requests.
			1. **Two ways govt can conduct surveillance under FISA**:
				1. **US Attorney General**: approves surveillance for **up to 1 year** if there is **no substantial likelihood of intercepting communications of US persons**
				2. **FISC**: approves **surveillance** that may involve **US persons** if there is **probable cause** to believe that **person is the agent of a foreign power** – must be renewed every 90 or 120 days
			2. **Wiretaps**: **DoJ must apply to FISC to obtain warrant authorizing electronic surveillance of foreign agents**. For targets that are U.S. persons, FISA requires heightened requirements in some instances. Agents must demonstrate probable cause to believe “target of the surveillance is a foreign power or agent of a foreign power,” that “a significant purpose” of surveillance is to obtain “foreign intelligence information,” and appropriate “minimization procedures” are in place.
				1. **No need to demonstrate** commission of **crime is imminent**.
				2. **Agents of foreign powers** include agents of **foreign political organizations and groups** engaged in **international terrorism**, as well as agents of **foreign nations**.
				3. President may authorize electronic surveillance to acquire foreign intelligence information for periods of up to 1 year without FISC order where US AG certifies “no substantial likelihood that the surveillance will acquire the contents of any communication to which a U.S. person is a party,” provided surveillance directed solely at communications among or between foreign powers, or “acquisition of technical intelligence … from property or premises under open and exclusive control of foreign power.”
				4. Due to secrecy of govt surveillance of agents of foreign powers, **entities that receive FISA order to produce records generally cannot disclose that fact to the targets of investigation**.
				5. **Companies are allowed to publish statistics about the number of FISA orders and NSLs they receive**
			3. **E-mails and stored records**: Where govt **accidentally intercepted** communications that “under circumstances in which a person has a **reasonable expectation of privacy** and a **warrant would be required** for law enforcement purposes, and if **both sender and intended recipients** are located in US,” government is required to destroy those records, “unless AG determines that contents indicate threat of death or serious bodily harm to any person.”
			4. **National Security Letters**: category of subpoena that, prior to the Patriot Act, was used narrowly, only for certain financial and communication records of an agent of foreign power and only with approval of FBI headquarters. **Patriot Act expanded use of NSLs**.
				1. Issued by authorized officials, Special Agent in Charge of FBI field office
				2. **Can be issued w/o judicial involvement** but under 2006 amendments recipients can petition federal court to modify or set aside NSL if compliance would be unreasonable or oppressive
				3. NSL can seek records relevant to protect against international terrorism or clandestine intelligence activities
				4. Patriot Act originally included strict rules against recipient disclosing receipt of an NSL (see below). 2006 amendment to Patriot Act said that recipients are bound by confidentiality only if there’s a finding by requesting agency of interference with criminal or counterterrorism investigation or for other listed purposes. **Recipients could petition court to modify or end secrecy requirement**. **Recipients were allowed to disclose request to those necessary to comply with the request and to an attorney for legal assistance**.
				5. **As of 2015**, FBI now presumptively **terminates NSL secrecy** for an individual order **when** an **investigation closes or no more than 3 years after full investigation opened**.
		2. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA-Patriot Act)**: **attacks of September 11, 2001 led to important changes to FISA, as part of the Patriot Act passed** in the wake of attacks.
			1. Amended FISA and ECPA - **Loosened requirements for surveillance of US persons** suspected of terrorist activities
			2. **Created “roving” wiretaps** - allowed investigators to get wiretap order against a person that was **valid for** **any type of communication** they engaged in, rather than requiring that the wiretap order specify the communications providers involved
			3. **Strengthened** **BSA** **rules against money laundering** and required that banks take steps to make sure that they know who owns the funds stored in their accounts
			4. **Expanded definition of pen register/trap and trace** beyond telephone numbers to include dialing, routing, addressing, or signaling info
			5. **Expanded Use of National Security Letter (NSL) under FISA** as **investigative tool to secretly demand records from communication services provider** – administrative subpoena that can be issued by FBI w/o involvement of a federal judge. Authority to issue NSL shifted from director of FBI to agents in charge of FBI field offices
			6. **Section 217**: Law enforcement officer needs to have court order or some other lawful basis to intercept wire or electronic communications. Owner or operator of computer system can face penalties under ECPA for providing access to law enforcement without following legally mandated procedures.
				1. **Permits, but does not require**, owner or operator of computer system to provide **access** in defined circumstances. **For computer trespassers** (i.e., hackers), **law enforcement can now perform interceptions** **if**:

The owner or operator of protected computer authorizes interception of 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 contents of computer trespasser’s communications will be relevant to the investigation

The interception does not require communications other than those transmitted

* + - 1. **Section 215**: Provides that federal court order can require **production of** **records or** **any tangible items** (including **call detail records**, books, other records, papers, documents or other items) **related to terrorist investigation**
				1. Recipients of the order are prohibited from disclosing the existence or contents of the order
				2. Disclosure of the order is permitted only to: **persons necessary** (e.g., employees who gather records) to comply with order **and** an **attorney for purpose of receiving legal advice**
		1. **FISA Amendment Act of 2008**. Gave legal authorization to new surveillance practices, especially where one party to the communication is reasonably believed to be outside of the US. It granted immunity to the telephone companies so they wouldn’t be liable for records provided to the govt in the wake of 9/11. Required more reporting from govt to Congress and put limits on some of the secrecy around NSLs and other requests for records relating to national security.
		2. **The USA Freedom Act of 2015**: **Enacted following Snowden revelations** and release of thousands of classified docs to the media that detailed govt programs re: collecting large amounts of info on citizens and non-citizens.
			1. Reformed US intelligence and surveillance laws and increased transparency of the FISA Court and added new controls to improve oversight of govt surveillance
			2. **Eliminated Section 215 – bulk collection of call detail records**
				1. Prohibited blanket “tangible things” production orders - **targeted warrants from FISA Court** **needed to collect phone metadata from telecom companies**
				2. Required use of **specific selector terms** such as when requesting records for specific phone number or email address under Patriot Act or for pen register/trap and trace orders issued under FISA
			3. **Judge must approve FISA orders for ongoing collection of records** except where US AG declares emergency
			4. **Changes to FISA Court**
				1. Court must obtain **independent expert opinions** when court believes govt surveillance application presents novel or significant interpretation of the law or in other cases where the court needs technical expertise
				2. Allows court to ask SCt to review questions about interpretation of the law
				3. Requires that Director of National Intelligence conduct **declassification reviews** of significant FISA Court orders and disclose those orders to the public when possible
			5. **NSLs must now  include specific selection terms** and there are **stricter requirements** on federal agencies **about when gag orders can be imposed on NSL recipients**. Recipients of NSL allowed to **challenge the letter or a gag order contained in the letter** **in court** and more disclosure of information about those letters is allowed.
			6. **Transparency** **Reports**: govt must issue **annual** transparency reports that include details on requests made using the National Security Authorities provided by USA Freedom Act
			7. **Companies** permittedto **publish aggregate info about FISA orders and NSLs** receivedin given period
		3. **The Cybersecurity Information Sharing Act of 2015 (CISA)**: permits the federal government to share unclassified technical data and information with private sector about how networks have been attacked and how successful defenses against such attacks have been carried out. Specific provisions include:
			1. Authorizes sharing or receiving “cyberthreat indicators” or “defensive measures” between govt and private sector **for a “cybersecurity purpose.”**
			2. **Requires redaction of PI not relevant to the threat before sharing**. For sharing to qualify for protections under CISA, the company’s actions must be done in accordance with certain requirements. For example, a company intending to share a “cyberthreat indicator” must first remove, or implement a “technical capacity” configured to remove, any information that is not directly related to a threat and that the company is aware at the time relates to a specific individual.
			3. Sharing information with federal government **does not waive privileges**, such as attorney-client privilege. Importantly, there is **no similar provision for sharing with state and local governments or other companies**.
			4. Shared information **exempt from federal, state and local FOIA laws** (i.e., laws “requiring disclosure of information or records).”
			5. **Prohibition on government using shared information to regulate or take enforcement actions against lawful activities**. Information shared under CISA “shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities related to monitoring, operating defensive measures, or sharing cyberthreat indicators.” The information may be used, however, to develop or implement new cybersecurity regulations.
			6. **Allows company to conduct security monitoring of its own info systems**. Company is authorized to “monitor” and “operate defensive measures” on its own information system or, with written authorization, another party’s system, for cybersecurity purposes.
			7. **Protection from legal liability for monitoring activities**. However, no corresponding liability protection for operating defensive measures.
	1. **CIVIL LITIGATION AND PRIVACY (0-2 QUESTIONS)**
		1. **Compelled disclosure of media information**: ***Zurcher v Stanford Daily (1978)*** – SCOTUS held that valid search warrants “may be used to search any property” where there is probable cause to believe that evidence of a crime will be found.
			1. **Privacy Protection Act of 1980 (PPA)**: Provides **extra layer of protection** for members of **media** and media organizationsfrom **government searches or seizures** in the course of **criminal investigation**.
				1. **Applies to Disseminators of Info to the Public and protects work product and documentary materials from search warrants**: Govt officials engaging in criminal investigations not permitted to search or seize media work product or documentary materials possessed by a person “reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast or other similar form of public communication, in or affecting interstate or foreign commerce.”
				2. **Government Agents Seeking Materials from Journalists and News Media** organizations must do so by obtaining **voluntary cooperation or a subpoena** that **may be contested in court** rather than using search and seizure powers
				3. But this **does not affect the govt’s ability to search for or seize such materials if**

there is **probable cause** to believe that the **person possessing the materials** has committed or is committing the **criminal offense to which the materials relate** if the offense is not the receipt, possession, communication, or withholding of such materials or the information contained therein or

there is **reason to believe** that the **immediate seizure** of such materials is **necessary** **to prevent** the **death of, or serious bodily injury** to, a human being

* + - * 1. PPA effectively **forces law enforcement to use subpoenas or voluntary cooperation** to obtain evidence from those engaged in First Amendment activities
				2. PPA applies to government officers or employees at all levels of government. Applies **only to criminal investigations**, not to civil litigation. Several states provide additional protections.
				3. Violation can lead to penalties of a minimum of $1,000, actual damages, and attorney’s fees.
				4. PPA was drafted to respond to police physical searches of traditional newspaper facilities. Going forward, courts may face claims that PPA is significantly broader, because **disseminating “a public communication” may apply to blogs, other web publishing, and perhaps even social media**.
		1. **Electronic discovery (electronically stored information (ESI))**: E-discovery implicates both domestic privacy concerns and issues arising in transborder data flows.
			1. **3 Major Steps in E-Discovery Process**: primarily owned by attorneys but privacy pros often assist
				1. **Preservation**: When an organization receives notice of potential litigation, the first step that should take place is the issuance of a legal hold to individuals and departments that may have electronic or paper records relevant to the dispute. Preservation includes more than not intentionally destroying information. When entity has reason to believe there will be litigation, all automated processes that would destroy relevant information must be suspended. Most often affects IT groups requiring preservation of log entries and ensuring that they are not automatically purged after a certain period of time or after the log reaches a certain size.
				2. **Collection**: of preserved electronic records – timing determined by attorneys – documents on file servers, files stored on individual computers, email messages stored on servers or in the cloud, and records in enterprise systems managed on prem or in the cloud. Must have processes in place to collect this information and will normally use e-discovery mgmt. product to assist with collection and organization of records.
				3. **Production**: records actually presented to the other side – the real heavy lifting begins. Review all collected records and decide which are relevant to the dispute and not protected by legal privileges (e.g., atty-client privilege). Electronic file with all relevant files shared with other side.
			2. ESI can be email, word processing documents, databases, web pages, server logs, instant messaging transcripts, voicemail systems, social networking records, thumb drives, or even microSD cards
			3. **Data Retention**: Managing e-discovery and privacy begins with a **well-managed data retention program**
				1. **Best practices for email retention** (Sedona Conference guidelines):

Email retention policies should be administered by **interdisciplinary teams** composed of participants across a diverse array of business units

The teams should continually develop their understanding of the policies and practices in place and **identify the gaps** between policy and practice

Interdisciplinary teams should reach consensus as to policies, while looking to **industry standards**

Technical solutions should meet and parallel the functional requirements of the organization

* + - * 1. **Good Faith Exception**: When done in good faith, data that is transitory, not routinely created or maintained for business purposes, and requires additional steps to retrieve and store may be outside the duty to preserve
				2. **Preservation and litigation hold**: even when wiping data is done within the normal course of business, in litigation, there is a **duty to act affirmatively to preserve the data**.
				3. **Conflict**: when corporate retention policy and discovery obligations conflict, **discovery obligations will likely prevail**. Courts apply **3-part test**:

Retention policy should be reasonable considering the facts

Court may consider similar complaints against the organization

Court may evaluate whether the org instituted the policy in bad faith

* + - 1. **Transborder data flows**
				1. Conflict between US obligation to follow discovery rules and, when data is located outside US, more restrictive laws in another country (e.g., GDPR in the EU)
				2. **Different approaches**

Plaintiff, seeking resolution in the U.S., needs to comply

All parties must comply; foreign statutes do not deprive an American court power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute.

Focus is on the nature or type of documents at issue; privacy log describing docs without disclosing contents

* + - * 1. **Conflict can be avoided by**:

**Hague Convention on the Taking of Evidence**: Party seeking to displace F.R.C.P. has burden of (1) demonstrating that it is more appropriate to use the Hague Convention and (2) establishing that the foreign law prohibits the discovery sought

Aerospaciale v. S.D. of Iowa provides factors a US court may use to resolve a conflict between US and foreign law re e-discovery requests:

Importance of the documents or data to the litigation

Specificity of the request

Whether the information originated in the US

Availability of alternative means of security for the info

Extent to which the important interest of the US and the foreign state would be undermined by an adverse ruling. (most important factor)

1. **WORKPLACE PRIVACY (8-12 QUESTIONS)**
	1. **OVERVIEW OF WORKPLACE PRIVACY (3-5 QUESTIONS)**
		1. **Workplace Privacy Concepts**: There is no overarching or organized law for employment privacy in the US. Federal laws apply in specific areas, such as to prohibit discrimination and regulate certain workplace practices, including employment screening and the use of polygraphs and credit reports. State contract and tort law in some instances provides protections for employees, but usually the employee must show fairly egregious practices to succeed. The regulation of employment privacy in the US stands in contrast with that in nations with comprehensive data protection laws, such as those in the EU.
			1. **Constitutional Law**: workplace privacy provisions apply only to federal and state government employees
				1. **4th Amdt**: prohibits unreasonable searches and seizures by state actors. Interpreted to place limits on ability of govt employers to search employees’ private spaces, such as lockers and desks.
				2. **State Constitutions**: some states, including CA, have extended right to privacy to private sector employees. Generally, though, if there’s no state action, no con law governs employment privacy.
			2. **State Contract, Tort, and Statutory Law**: Employer-employee relationship in the US is fundamentally a contract law issue – employment at will. **Employer discretion** to fire an employee understood to imply broad latitude in defining the employment relationship, including knowledge about the employee. Employees generally have narrow protections contract, tort and statutory law.
				1. **Contract**: can alter the rules between employer and employee – most important of which are collective bargaining agreements that are protective of employee rights.
				2. **Tort**: potential claims by employees include intrusion upon seclusion, publicity given to private life, and defamation, all of which provide possible privacy protections of very narrow scope.
				3. **State Laws**: vary enormously by state, leading to a patchwork of complexity and large gaps
			3. **Human Resources Management**: Organizations have to consider which jurisdiction’s rules apply to PI about particular employees. Companies with employees in the US and other countries must be aware that different workplace rules apply to employment privacy. For example, the EU includes employee privacy within its general rules applying to the protection of individuals and employees have broad workplace privacy expectations and rights. For multinational corporations, this can present challenges, such as when HR data systems in one country contain PI about employees residing in other countries, or when employees share PI across borders, such as through email or other channels. Equally true for employees that reside in different states in the US.
		2. **U.S. Agencies Regulating Workplace Privacy Issues**:
			1. **Federal Trade Commission (FTC)**: Enforces a variety of laws including **FCRA**, which limits employer’s ability to receive an employee’s or applicant’s credit report, driving records, criminal records and other **consumer reports** from a CRA in **reference checking** and **background checks** of employees
				1. When employer uses consumer reports to make employment decisions, including hiring, retention, promotion or reassignment, it must comply with FCRA
			2. **Department of Labor (DoL)**: Administers and enforces FLSA (wages and overtime pay), OSHA, ERISA (administration of retirement plans), the Employee Polygraph Protection Act (EPPA) (regulating use of lie detectors) and FMLA. Each state has an agency, often called the Department of Labor, that oversees state labor laws.
				1. **Occupational Safety and Health (OSH) Act**: administered by Occupational Safety and Health Administration (OSHA). Safety and health conditions in most private industries are regulated by OSHA or OSHA-approved state programs, which also cover public sector employers. Employers covered by the OSH Act must comply with the regulations and the safety and health standards promulgated by OSHA. Employers also have a general duty under the OSH Act to provide their employees with work and a workplace free from recognized, serious hazards. OSHA enforces the Act through workplace inspections and investigations. – **workplace safety**
				2. **OSHA enforces whistleblower protections in most laws**: Most **labor safety laws** and many environmental laws **mandate whistleblower protections for employees** who complain about violations of the law by their employers. Remedies can include job reinstatement and payment of back wages.
				3. **Employee Polygraph Protection Act of 1988 (EPPA)** – see below
			3. **Equal Employment Opportunity Commission (EEOC)**: responsible for enforcing **US Anti-Discrimination Laws** that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy, transgender status, and sexual orientation), national origin, age (40 or older), disability or genetic information, all of which protect employees from retaliation if they complain about discrimination or participate in an EEOC proceeding (for example, a discrimination investigation or lawsuit). **These anti-discrimination laws have sometimes been used to limit background checks and primarily prohibit discrimination in hiring and other employment decisions, but there’s often a collateral effect on how interviews and other background screening activities are conducted.** Most employees with **at least 15 employees** are covered by EEOC laws (20 employees in case of age discrimination). Most labor unions and employment agencies are also covered. The laws apply to all work situations, including hiring, firing, promotions, harassment, training, wages and benefits.
				1. Title VII of the **Civil Rights Act of 1964**: makes it illegal to discriminate against a person on the basis of **race, color, religion, sex** (including pregnancy, transgender status, and sexual orientation), **or national origin**.
				2. Titles I and V of the **Americans with Disabilities Act of 1990 (ADA)**: makes it illegal to discriminate against a **qualified person with a disability** in **private companies and state and local governments**. Has a broad definition of disability, covering not only individuals with actual disabilities but also those who have record of disability and those who are “regarded as” disabled by the employer. Predisposition to developing illness or disease is not a physical impairment (EEOC guidance) and therefore not covered by ADA. However, emerging trend is whether ADA protects potential future disabilities.

**Qualified Individual**: an individual who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires

**Essential Function**: those core duties that are **the reason the job position exists** – not marginal or incidental job functions

**Reasonable Accommodation** must be provided by employer to accommodate **known** disability of qualified applicant or employee **unless** can demonstrate **undue hardship on operation of the business**

**Reasonable Accommodation**: any modification or adjustment to a job, the job application process, or the work environment that will enable a qualified applicant or employee with a disability to participate in the application process, perform the essential functions of the job, or enjoy the benefits and privileges of employment.

Employee’s **1st choice** of accommodation **not required**

**Effective accommodation** is **required**

Employee need not disclose particular illness, but **employer can require medical documentation of disability and limitations**, so disclosure of illness or condition may be necessary during interactive accommodation process. **If medical information disclosed**, ADA requires **confidentiality** and info must be kept apart from general personnel files in a **separate, confidential medical file** available only under limited conditions.

**Undue Hardship**: action that requires **significant difficulty or expense** in relation to size of employer, resources available and nature of the operation. Customer or co-worker attitudes are not relevant factors in determining undue hardship – potential loss of customers or co-workers doesn’t constitute undue hardship

**Examples of Reasonable Accommodation**:

making existing facilities readily accessible to and usable by employees with disabilities

restructuring a job

modifying work schedules

acquiring or modifying equipment

reassigning a current employee to a vacant position for which the individual is qualified

**Present Not Future Ability to Do Job**: Employers cannot fire or not hire qualified person because of fear person will become too ill to work in the future. Hiring decision must be based on how individual can perform at present time.

**Higher Costs**: Higher medical insurance costs, workers’ comp costs or potential absenteeism are not permissible reasons not to hire qualified person with disability

**Health & Safety**: ADA permits **qualification standards** that **exclude individuals who pose a direct threat**—i.e., a **significant risk of substantial harm** — established through objective, medically-supportable methods (not simply assumed to exist) to the health or safety of the individual him/herself or to the safety of others, **if** that **risk cannot be eliminated or reduced** below the level of a “direct threat” by reasonable accommodation

**ADA Amendments Act of 2008 (ADAAA)**: significantly expanded scope of ADA protections by broadly defining disabilities to include 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**. Obesity is not a disability unless the weight gain is caused by an underlying physical condition but severe or morbid obesity (100% more than normal body weight) is a disability (i.e., if it substantially limits the person’s ability to walk, stand, kneel, stoop and breathe). Pursuant to ADAAA, EEOC released regulations addressing scope of ADA in 2011.

legislatively **overturned** two SCOTUS cases which limited scope of ADA – **Sutton v UAL** (held that pilots with severe but correctable myopia did not have a disability under the ADA because a “‘disability’ exists only where an impairment ‘substantially limits’ a major life activity, not where it ‘might,’ ‘could,’ or ‘would’ be substantially limiting if mitigating measures were not taken) and **Toyota v Williams** (held “an individual must have an impairment that prevents or severely restricts the individual from doing activities that are of central importance to most people’s daily lives. The impairment’s impact must also be permanent or long-term.”)

**BEFORE EMPLOYMENT OFFER**

ADA restricts **medical screening** of candidates **before offer of employment** - specifically covers “medical examinations and inquiries” as **grounds for discrimination** unless “job related and consistent with business necessity.”

**Job Related and Consistent with Business Necessity** means employer **must have reasonable belief based on objective evidence** that:

employee will be **unable to perform essential job functions** because of medical condition OR

employee will **pose direct threat** because of medical condition

During hiring process and before conditional offer, employer **may not ask** applicant **whether needs** **reasonable accommodation** for the job, **except** when employer knows applicant has disability, but can ask applicant during interview about ability to perform job functions.

**AFTER (CONDITIONAL) EMPLOYMENT OFFER**

Medical exam may be required **after offer of employment,** and may condition offer on the results, **only if**:

all entering employees subject to exam regardless of disability

confidentiality rules followed for results of exam, and

results used only according to laws against discrimination on basis of disability (i.e., job-related and consistent with business necessity)

After conditional offer, employer may inquire whether applicant needs reasonable accommodation **if** all entering employees in same job category asked this question.

**After person starts work**, med exam or inquiry must be **job-related and consistent with business necessity** (e.g., where there’s evidence of job performance or safety problem, exam required by other Federal laws or when exam necessary to determine current fitness to perform particular job)

**Prohibited Pre-Hiring Practices**:

No questions about **prior injuries and illnesses**, including **prior worker comp claims**

**Psychological tests** (e.g., to predict conditions such as depression or paranoia) might qualify as medical exams

No questions about **recovery from drug addiction or alcoholism** even though ADA does not cover use of alcohol or drugs

Employers should stay away from pre-hire inquiries about likelihood that candidate has covered disability or whether will seek reasonable accommodation

* + - * 1. Title II of the **Genetic Information Nondiscrimination Act (GINA)**: makes it illegal to discriminate against employees or applicants because of **genetic information**. Genetic information includes information about an individual's genetic tests and the genetic tests of an individual's family members, as well as information about any disease, disorder or condition of an individual's family members (i.e., an individual's family medical history).
			1. **National Labor Relations Board (NLRB)**: administers the **National Labor Relations Act (NLRA)** and investigates and remedies unfair labor practices by employers and unions. The NLRA **protects the rights of employees to act together to address conditions at work, with or without a union**. Generally, concerted activity with other employees is protected. This protection extends to certain work-related **social media communications** (e.g., conversations conducted on social media platforms), but not if the social media communication does not involve fellow employees.
				1. **2010**: NLRB started receiving complaints related to **employer social media policies and discipline** for FB postings. Some policies violated federal labor law and NLRB GC issued complaints against employers alleging unlawful conduct. In other cases, investigations found that communications were not protected, so disciplinary actions taken by employers did not violate NLRA.
				2. **NLRB Jan 2012 Report**: two main points about NLRB and social media

Employer policies **should not** be so sweeping that they **prohibit** the kinds of activity protected by federal labor law, such as the **discussion of wages or working conditions** among employees

Employee’s comments on social media are generally not protected if they are **mere gripes not made in relation to group activity among employees**

* + - 1. **Securities and Exchange Commission (SEC)**: **requires reporting of human resources information** (e.g., payment/salary and other information about senior executives**)** by publicly traded companies to the govt and to the public.
	1. **PRIVACY BEFORE, DURING AND AFTER EMPLOYMENT (5-7 QUESTIONS)**
		1. **Employee Background Screening**: Certain professions are subject to background screening by law. **Anyone who works with the elderly, children or the disabled must now undergo background screening**. EEOC cautions businesses to carefully review background screening processes, such as denying employment based on criminal convictions, to ensure that requirements are job related and necessary. **Searches of publicly available information generally considered reasonable practice in US**. Significant privacy issues can accompany such practices.
			1. **Requirements Under FCRA**: regulates how employers perform any type of **background check / consumer report** on a job applicant obtained from a CRA, including credit checks, criminal records, and driving records. Under FCRA, “consumer report” includes all written, oral or other communications bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living. FTC has aggressively enforced **FCRA violations** against nontraditional CRAs who collect data online without using reasonable procedures to ensure maximum possible accuracy of information being sold and report it to employers result in large civil penalties.
				1. FCRA permits employers to obtain

**consumer report** for

**pre-employment screening** for the purpose of evaluating the candidate for employment

determining if an existing employee qualifies for **promotion, reassignment or retention**

**investigative consumer report** on an applicant for permissible purposes (i.e., using the information for employment purposes)of

* + - * 1. **Employer must** meet following standards **to obtain any type of consumer report**:

Provide **written notice to applicant** that obtaining consumer report for employment purposes and indicate if investigative consumer report will be obtained

Obtain **written consent from applicant** (original consent can be used to get updates as needed)

Obtain data only from **a qualified CRA**, an entity that has taken steps to assure the accuracy and currency of the data

**Certify to CRA** that the employer has a **permissible purpose** and has obtained **consent** from the employee

Before taking adverse action, such as denial of employment, provide **pre-adverse-action notice** to applicant **with a copy of consumer report**, to give applicant opportunity to dispute report

After taking adverse action, provide **adverse action notice**

**Non-compliance** with the above can result in **civil and criminal penalties**, including **private right of action**

* + - * 1. There are no obligations under FCRA when an employer does not use a CRA and conducts its own background check.
				2. FACTA amendments to FCRA preempted many state laws on credit reporting, identity theft and other areas of FCRA, but **FCRA does not preempt** states from creating **stricter legislation** regarding **employment background checks**. Notable among them, the **California Investigative Consumer Reporting Agencies Act (ICRAA)**

**Under ICRAA,** unlike FCRA, the law requires **new written consent each time** a consumer report is sought during employment if the report is for purposes other than suspicion of wrongdoing or misconduct - employers must notify applicants and employees of intent to obtain consumer report, must obtain employee’s written consent to obtain the report and enable employee to request a copy of the report **every time** a background check is conducted. Any **adverse action must result in copy of report to employee**, regardless if waived right to receive copy of the report. **Notice and consent rules don’t apply if employee suspected or wrongdoing or misconduct**.

**When California employers conduct their own background checks** without contracting 3rd party, some provisions of ICRAA apply but not all.

Employer must give employee or applicant a **copy of any** **public records** resulting from in-house background check unless employee waives the right

If adverse action results, must give employee or applicant copy of public records regardless of waiver

**In-house reference checks** – no requirement to give info to employee or applicant

**10 other states limit use of credit information in employment -** Colorado, Connecticut, Delaware, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont and Washington – in these states, **credit history can only be used if related to the position applied for**.

* + - 1. **Methods**
				1. **Personality and Psychological Evaluations**: EPPA and ADA together place significant federal limitations on psychological testing (e.g., lying and impairment of mental health) in the workplace, but **employers still use psychological tests for personality traits (e.g., honesty, preferences and habits)**
				2. **Polygraph Testing**: **Employee Polygraph Protection Act of 1988 (EPPA)** prohibits most private employers from using lie detector tests, or the results of such tests or any refusal to take such tests, for pre-employment screening or during the course of employment. **Employer must post essential provisions of EPPA in a conspicuous location** so employees aware.

**Lie Detector** – polygraphs, voice stress analyzers, psychological stress evaluators, or **any similar device** used to render **diagnostic opinion** regarding individual’s **honesty**

**Exceptions**:

Subject to restrictions, polygraph tests (a type of lie detector) can be administered to **certain job applicants**

**Govt employees**

**Security service firms** (armored car, alarm, and guard)

**Pharmaceutical** (controlled substances) manufacturers, distributors and dispensers

**Defense contractors**

National security functions

In connection with **ongoing investigation** involving **economic loss or injury** **to** the **employer’s business** (theft, embezzlement, industrial espionage) if have **reasonable suspicion –** no discharge because of results or refusal unless **additional supporting evidence**.

**Enforcement**: fines from **DoL** as well as **private right of action**

**No preemption of stricter state law**

* + - * 1. **Drug and Alcohol Testing**: **No federal privacy statute** that directly governs employer testing of employees for substances such as illegal drugs, alcohol or tobacco

For **public-sector employees** – **4th Amdt case law** on when substance use testing is reasonable

**Illegal Drug Use**: **current use not protected** **by ADA** and excluded from definition of “individual with a disability,” and **drug test not considered medical exam**

**History of Illegal Drug Use**: Casual drug use is not a disability under the ADA. Drug addiction considered disability under ADA **if** poses substantial limitation on one or more major life activities **and** person not currently using illegal drugs.

Denying job because of history of casual drug use would not violation of ADA

Policies that screen out applicants because of history of addiction or treatment for addiction must be job-related and consistent with business necessity

Current illegal drug use, even if addicted, can be denied employment because of current use

Asking job applicant if ever used illegal drugs or been arrested for using illegal drugs is **not** violation of ADA

Asking about **prescription drug** **use** permitted in response to positive drug test, even if answers may disclose information about disability

**Alcohol Use**: **current use not automatically denied protection** **under ADA**. Alcoholism(alcohol use disorder)is protected as a disability **if person qualified** to perform **essential job functions – BUT**- employer can

**discipline, discharge or deny** employment **if** **alcohol use adversely affects** job performance or conduct

**prohibit alcohol use in workplace**

require that employees are **not under the influence** of alcohol **while at work**

**Federal Law** mandates **drug testing for certain positions** in the federal sector (e.g., US Customs & Border Protection) and creates regulations for drug testing for employees in certain sectors - **aviation, railroading and trucking** **industries, which preempt state laws that would otherwise limit drug testing**. Because marijuana is federally prohibited, employees in these industries must adhere to federal requirements.

**Permissible Reasons for Drug Testing:**

**Pre-employment** - if not designed to identify legal use of drugs or addiction to illegal drugs

**Reasonable suspicion** - as a condition of continued employment if “reasonable suspicion” of drug or alcohol use based on specific facts and rational inferences from those facts (e.g., appearance, behavior, speech, odors)

**Routine testing** - if employees **notified at time of hire**, unless state or local law prohibits it

**Post-accident testing** - as a condition of continued employment if “reasonable suspicion” that employee involved in accident was under influence of drugs or alcohol

**Random testing** - sometimes required by law, prohibited in certain jurisdictions, but acceptable where used on existing employees in specific, narrowly defined jobs, such as those in highly regulated industries where the employee has a severely diminished expectation of privacy or where testing is critical to public safety or national security

* + - * 1. **Social Media**: Employers are legally permitted to use social media in informing their decisions but **can’t violate anti-discrimination and privacy laws**. Employers face risks when engaging in **social engineering** - use of manipulation to gain access to otherwise private information, including connecting with potential hires or employees through false online profile or requesting access to private networks not available to general public. These practices can results in **invasion of privacy actions** for violating applicant’s or **employee’s reasonable expectation of privacy**. Employers can screen publicly available social media sites on their own because FCRA doesn’t prohibit DIY background checks, but if use 3rd party, must be qualified CRA that has ensured maximum possible accuracy of the information. **Employers should not require current employees to divulge access information to private networks as a condition of employment.** Some states have made it illegal to ask an applicant or employee for their social media login information and passwords – Maryland was the first in 2012 and, as of 2019, 25 more states have done the same and Congress has proposed similar legislation.
		1. **Employee Monitoring**: In US, private-sector employees have limited expectations of privacy at workplace. Physical facilities belong to employer, and employer in private sector has broad legal authority to monitor and search workplace. **Formal policies about workplace monitoring and accompanying documents may be required by state law for monitoring to be lawful**. Providing employees with notices of these policies helps establish their knowledge and reasonable expectations about workplace activities.
			1. **Technologies**: Federal and state laws regulate and restrict workplace surveillance activities, including video surveillance, monitoring of telephone calls, and electronic surveillance, such as accessing emails and monitoring internet activities.
				1. **Computer Usage (including Social Media)**: Invasive monitoring practices may provide basis for discrimination lawsuits if employer accesses and appears to use legally protected information, including religion, ethnicity, gender or sexual orientation, political affiliations, and other sensitive information, all of which is commonly available on individuals’ social media pages. Although reading publicly available information is lawful, discriminatory actions and invasions of privacy in the workplace – such as monitoring information about an employee on social medial sites - are not.
				2. **Biometrics**: Biometric information privacy laws in place in different states throughout the country typically require specific disclosures be made to employees prior to collection, use, or storage of biometric data and carry heavy penalties for employers who fail to do so.

**Illinois Biometric Information Privacy Act (BIPA)** is the forerunner of modern US biometric information privacy laws.

**CCPA**: regulates collection, storage, and use of “biometric information,” defined broadly

**Texas and Washington**: prohibit unauthorized collection and use of ‘biometric identifiers’

**4th Cir “Mark of the Beast” Case (EEOC v. Consol Energy)**: held that when combine sincerely held religious belief with conflicting employment requirement (biometric time clock), employer is obligated to consider religious accommodation.

* + - * 1. **Location-Based Services (LBS)**: Mobile phones, GPS devices, and some tablet computers provide geolocation data, which enables tracking of the user’s physical location and movements. **Employers can monitor location of company vehicles equipped with GPS if monitoring is for business purposes during work hours and employee informed beforehand**. Some state laws limit monitoring of geolocation data of employees themselves to an extent. **CT requires written notice for any type of electronic employee monitoring** and civil penalty for violations. **CA has outlawed use of “electronic tracking devices to determine the location or movement of a person.”** Use of LBS to monitor employees runs risk of invasion of privacy claims where employee has reasonable expectation of privacy.
				2. **Wellness Programs**: **Employee must provide written consent and participate voluntarily**. If wellness program offered as part of company’s group health insurance plan, PII collected from or created about participants in program is PHI and protected by **HIPAA privacy rule**. HIPAA also protects PHI held by employer as plan sponsor on the plan’s behalf when the plan sponsor administers aspects of the plan, including wellness program benefits offered through the plan. Wellness programs offered directly by employer and not as part of group plan are not covered by HIPAA. **ADA** (applies to wellness programs that ask for medical info or require medical exams of employees - **wellness programs must be voluntary because they’re not job related**), **GINA** (applies to wellness programs that ask for medical info or require medical exams of employee spouses – **exception where employee/family member consents in writing and voluntarily participates in health or genetic services (i.e., wellness programs)** **if related info kept confidential**) and **state laws** apply regardless of HIPAA coverage.
				3. **Mobile Computing – Bring Your Own Device (BYOD)**: employees use their personal computing devices for work purposes, which presents security challenges stemming from lack of employer control over employee devices as well as workplace privacy issues. Employee expectations of privacy in BYOD context likely higher because personal device involved. **Surveillance and monitoring** activities used for work-issued devices may not be appropriate for personal devices. Employers should clearly address issues and convey to employees privacy limits and risks when using personal devices in workplace. If employer engaged in device monitoring or surveillance, it should **disclose** that information and **obtain employee consent**. When monitoring and searching the device, **exposure of private employee data should be minimized**.
				4. **Postal Mail**: Federal law prohibits interference with US mail delivery. Mail is considered “delivered,” however, when it reaches a business. Opening business letters and packages by a company does not violate statute, even if the rep is not intended recipient. **But** state common law might present risk (confidentiality of personal information).
				5. **Stored Communications**

**The Stored Communications Act (SCA)** creates general prohibition against unauthorized acquisition, alteration or blocking of electronic communications while in electronic storage in facility through which electronic communications service provided. **Employer Exceptions if conduct authorized**:

“By the person or entity providing a wire or electronic communications service” (often the employer)

“By a user of that service with respect to a communication of or intended for that user”

Employers permitted to look at workers’ electronic communications if employer’s reason for doing so is **reasonable and work related**

* + - * 1. **Photography**: Federal law doesn’t limit use of photography in workplace areas, but **state statutes and common law** create limits in some settings – e.g., common areas, such as break rooms, restrooms, locker rooms, and places where employees change clothes.
				2. **E-Mail and Telephony**: **Wiretap Act and ECPA prohibit** interception of wire communications (**nonconsensual surveillance**), such as phone calls or sound recordings from video cameras; oral communications, such as hidden bugs or microphones; and electronic communications, such as emails. **Unless exception applies**, interception of these communications is **criminal** **offense** and provides **private right of action**. **Exceptions**:

Person is party to the call or **one of the parties consents** to the interception

Interception done in the **ordinary course of business** (reasonably related to a business purpose)

Employer who provides communication services, such as a company telephone or email service, can intercept if **employee consents** **or** interception occurs in **normal course of user’s business**.

* + - * 1. **Video**: Cameras and video recordings **w/o sound recordings** are **outside scope of federal wiretap and stored-record statutes**. Federal law doesn’t limit use of video cameras in workplace areas, but **state statutes and common law create limits in some settings** – e.g., common areas, such as break rooms, restrooms, locker rooms, and places where employees change clothes. **Closed-circuit TV (CCTV), security cameras and other video surveillance are permitted in workplace common areas** that generally wouldn’t be considered “private places” that might be considered offensive or an invasion of privacy.
			1. **Requirements under the Electronic Communications Privacy Act of 1986 (ECPA)**: Encompasses both the Stored Communications Act (SCA) and the Wiretap Act (the federal Wiretap Act is a one-party consent statute). No preemption of stricter state privacy laws. Some state laws protect email communications.
				1. ECPA provides that **employer may not record** telephone conversations **unless one of the following** exceptions applies:

**Consent**: employer can monitor or intercept employee communications if employee consents to the surveillance - consent satisfied, or at least implied, where **employee notified** that calls are being recorded, **or** has expressly given consent pursuant to **employment contract or company policy**

Employers should **notify and forewarn** employees that **calls may be recorded** and that have **limited expectation of privacy in workplace**

**Business Extension or Business Use**: Wiretapping permitted to monitor, intercept, and record employee’s conversations without employee’s consent when employee uses **employer’s phone system** and call is **work-related**, including to protect trade secrets or ensure compliance with non-compete agreements. Also, if employer has reasonable suspicion that employee engaged in misconduct or violating company policy, employer can justify recording work-related calls.

surveillance of employee personal phone calls beyond point of determining whether work-related (or not) is outside “the ordinary course of business” and prohibited by Wiretap Act

general policy of monitoring employee calls does not legitimize wholesale surveillance of employee calls or establish that all calls occur in ordinary course of business - **each act of surveillance must be reasonably business-related**

* + - * 1. ***City of Ontario v Quon***: SCOTUS held that government employer’s search of police officer’s personal and work-related text messages on employer-issued pager was reasonable and officer’s 4th Amdt rights not violated. Even through private employers not subject to prohibition on warrantless searches like govt employers, all employers should ensure electronic communications policies meet current norms in specific workplaces and should educate employees about policies.
				2. **Best Practice - Employer Monitoring Policy**: Employers seeking to intercept, record or monitor employee phone calls should establish and disseminate to employees **clearly written company policies**:

phone calls may be subject to monitoring and surveillance without further warning

expressly state that no obligation to monitor employee communications – to avoid claims of failure to protect from or investigate misconduct or other harm

require employees to sign written acknowledgment that received, read and understood policies, and agree to abide by them as a condition of employment

policies should be reaffirmed by employees periodically in ordinary course of business

* + - 1. **Unionized worker issues concerning monitoring in the U.S. workplace**: NLRB held that **surveillance of any portion of workplace** is condition of employment that **must be the subject of collective bargaining** and **agreed to by union prior to implementation**.
		1. **Investigation of employee misconduct**: Employer’s typically conduct workplace investigations of employee misconduct for (1) discrimination or harassment, (2) threat of violence, (3) theft, embezzlement or fraud, or (4) controlled substances.
1. **Best Practices**:
2. Take allegations seriously
3. Treat employees fairly
4. Follow laws, corporate policies and collective bargaining agreements
5. Document alleged misconduct
6. Consider rights of other employees and 3rd parties
7. **Data handling in misconduct investigations**: Document alleged misconduct and investigation to minimize risks from subsequent claims by employee. All information related to the investigation should be kept strictly confidential. Investigations involve handling PI of employee under investigation, witnesses and other 3rd parties. Must comply with data privacy laws.
8. **Use of third parties in investigations**: FACTA amended the FCRA to address problems created by the FTC’s “**Vail Letter**” (1999 FTC staff opinion letter concluding that FCRA regulates workplace misconduct investigations conducted by third parties, which would require employee consent for the related “investigative consumer report”).
9. **FACTA nullifies Vail Letter** by **excluding from definition of consumer reports misconduct investigation reports** and investigation reports into “compliance with Federal, State, or local laws and regulations, the rules of a self-regulatory organization, or any preexisting written policies of the employer.”
10. **Adverse Action**: If employer takes adverse action on basis of report, **FACTA requires** employer to disclose **summary of nature and substance of report to employee**, which can be issued after investigation completed to maintain secrecy of investigation. Does not prescribe amount of information that must be disclosed but permits exclusion of “**sources of the information** acquired solely for use in preparing [the report],” e.g., the names of any witnesses.
11. **Documenting performance problems**: Progressive and documented discipline for initial or minor infractions can provide a reasoned basis for more serious discipline or termination if necessary. Work with compliance department to determine appropriate level of documentation.
12. **Balancing rights of multiple individuals in a single situation**: Consider rights of people other than those being investigated, such as fellow employees/witnesses who could be subject to retaliation or other problems. Witnesses have an ongoing duty to keep all information relevant to the investigation and their own statements strictly confidential and not to discuss this internally or externally. Witnesses need to be assured that can give evidence w/o detrimental treatment or penalty for participating in investigation.
	* 1. **Termination of the employment relationship**: terminating access to company’s physical and informational assets, and proper HR practices post-employment
			1. **Transition management**: clear procedures for terminating access to facilities and information. IT systems designed to minimize disruption when person no longer has authorized access. **Basic steps include**:
				1. Secure the return of badges, keys, smartcards and other methods of physical access
				2. Disable access for computer accounts
				3. Ensure the return of laptops, smartphones, storage drives and other devices that may store company information
				4. Seek, where possible, to have the employee return or delete any company data that is held by the employee outside of the company’s systems
				5. Remind employees of their obligations not to use company data for other purposes
				6. Clearly marked personal mail, if any, should be forwarded to the former employee, but work-related mail should be reviewed to ensure that proprietary company information is not leaked
				7. Remind employees during their exit interview of their ongoing confidentiality obligations under their NDA
			2. **Records retention**: appropriate practices for maintaining HR records of former employees - to provide references, respond to inquiries about benefits and pensions, address health and safety issues that arise, respond to legal proceedings, and meet legal or regulatory retention requirements for particular types of records **balanced against** privacy and security of sensitive employment records
			3. **References**: common law imposes no duty on former employer to supply reference for former employee. Some state statutes require references for specific occupations (pilot, public school teacher). Benefit of goodwill with former employees needs to be balanced against risk of suit for defamation.
		2. **Working with third parties**:
13. **STATE PRIVACY LAWS (5-7 QUESTIONS)**
	1. **FEDERAL VS. STATE AUTHORITY** **(0-2 QUESTIONS)**
		1. **Federal Preemption**
			1. Privacy advocates historically have either opposed preemption or sought to narrow whatever preemption exists - state privacy law innovation has often been an important step toward eventual federal privacy protections
			2. Industry usually insists that preemption is essential to passage of any general federal privacy law - compliance becomes more expensive when there is a “patchwork” of state laws
			3. Subject matter preemption vs Field preemption
			4. **Most federal privacy laws DO NOT preempt stricter state privacy laws** on the theory that privacy laws exist to protect individual rights, and states should have the ability to offer greater protection of rights to their citizens
				1. HIPAA
				2. GLBA
				3. Electronic Communications Act (ECPA)
				4. Right to Financial Privacy Act (RFPA)
				5. Cable Communications Policy Act
				6. Video Privacy Protection Act (VPPA)
				7. Employee Polygraph Protection Act (EPPA)
				8. Telephone Consumer Protection Act (TCPA)
				9. Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFPA) (Do Not Call)
			5. **3 Major federal privacy laws DO preempt stricter state privacy laws**
				1. **Children’s Online Privacy Protection Act of 1998** (**COPPA**) **but** no effect on state law ages 13-18

Preempts “inconsistent State law” where COPPA rules apply and not otherwise

* + - * 1. **CAN-SPAM** Act (2003) – preemption **where *expressly regulates the use of electronic mail to send commercial messages***, except to the extent that any such statute, regulation, or rule prohibits *falsity* or *deception* in any portion of a commercial electronic mail message or information attached thereto

The gap between the narrow scope of CAN-SPAM and the broad scope of proposed federal privacy bills today hints at the challenges of writing an effective preemption provision

* + - * 1. **FCRA and FACTA –** very complex preemption mechanism **-** state laws generally still apply, except where the FCRA has a specific preemptive effect
	1. **MARKETING LAWS (0-2 QUESTIONS)**
	2. **FINANCIAL DATA (0-2 QUESTIONS)**
		1. **Credit history**: FCRA does not preempt states from creating stronger legislation in the area of employment credit history checks, such as **California ICRAA** (see p.58 above). **Ten other states - Colorado, Connecticut, Delaware, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont and Washington - limit use of credit information in employment.** These states **require that credit history information be used only as (substantially) related to the position applied for**. While most states require a substantial relationship, Hawaii requires the applicant’s credit history to directly relate to an occupational qualification. Additionally, some states allow credit history checks to be performed if the position applied for fits within predefined occupational categories, generally involving financial or managerial responsibility or exposure to confidential information.
		2. **California Financial Information Privacy Act (CFIPA) (aka California SB-1)**: expands financial privacy protections under GLBA
			1. Written **opt-in consent** is required for FI to share PI with **nonaffiliated 3rd parties**
			2. Opt-in must be presented on form called “Important Privacy Choices for Consumers” and written in simple English
			3. Grants consumers the right to **opt-out** of info sharing between FI and **affiliates not in same line of business** (not regulated by same functional regulator)
			4. CCPA specifically intends to avoid conflict with GLBA and CFIPA but the exemption applies to datasets and not to the organization that holds the data – **only the data (not the org) specifically covered by GLBA or CFIPA is exempt from CCPA**
	3. **DATA SECURITY LAWS (0-2 QUESTIONS)**

**Information privacy** concerns decisions about the authorized use and disclosure of PI and involves the data subject’s right to control the data, such as rights to notice and choice. **Information security** is the protection of information, whether it is personal or other types of information, from loss and unauthorized access, use and disclosure.

**Information Security** requires ongoing assessment of threats and risks to information and the procedures and controls used to protect information, consistent with the following:

* Confidentiality - access to data is limited to authorized parties
* Integrity - assurance that the data is authentic and complete
* Availability - knowledge that the data is accessible, as needed, by those who are authorized to use it

**Information security is achieved by implementing controls**, which need to be monitored and reviewed, to ensure that organizational security objectives are met. Security controls are mechanisms put in place to prevent, detect or correct a security incident. **3 types of security controls** are:

* Physical controls - locks, security cameras, and fences
* Administrative controls - incident response procedures and training
* Technical controls - firewalls, antivirus software, and access logs
	+ 1. **SSN**:
			1. **Digitization of consumer finance and the adoption of SSN as the keys to an individual's identity** now means that someone who obtains and Social Security number can use it to steal the person’s identity and impersonate them, both online and in the physical world. The sensitivity of SSNs causes significant challenges for organizations. Those who once used SSNs as unique identifiers may now have large stores of this data that puts the organization at risk. Some organizations, especially those involved in financial transactions and taxes, must continue to use SSNs to some extent, but they must implement strong security controls to secure this sensitive information.
			2. **Danger in using last 4 digits of SSN as an identifier** because for a long period of time (1987-2011) SSNs were issued in a very structured manner – [\*\*state - group #- serial # (unique identifier of an individual)\*\*]. Starting in 1987, SSNs were issued at birth instead of on an as-needed basis. These 2 issues mean that the first five digits of a Social Security number can be predicted on a fairly reliable basis for any number issued between 1987 and 2011. If you know someone's birthdate and the state where they were born, you can combine those last four digits with the prediction made by an algorithm, and you'll be correct about half the time (44%) for people born between 1987 and 2011.
			3. **Bottom Line**: organizations should **avoid using even the last four digits of SSNs**, unless absolutely necessary. If an individual was born between 1987 and 2011, they should protect the last four digits of their SSN as though it were the entire SSN.
			4. **There is no one law that governs the use of SSNs**. Many states have specific laws restricting or prohibiting the collection, use or disclosure of SSNs by commercial entities. These laws generally prohibit use of SSNs in a manner that provides public view or access, although many state laws provide exemptions for entities covered by federal legislation (HIPAA, GLBA, FCRA).
			5. **At least six states** - Connecticut, Massachusetts, Michigan, New Mexico, New York, and Texas - **impose additional requirements** for organizations to **develop policies to safeguard SSNs** and, in some instances, to make their **SSN protection policies** available to the **public** or to their **employees**.
			6. Some states prohibit use of the **entire number** but not a **truncated or redacted number**. Other states, like NY, are more restrictive (**SSN and anything derived from SSN with exception for encryption**).
			7. Various state **statutes prohibit** organizations from
				1. printing **SSN on consumer cards**
				2. sending **SSN through the mail**
				3. **requiring** that consumer **transmit SSN unencrypted over internet**
				4. **requiring** that individuals **use their SSN to access a website without multi-factor authentication**.
			8. Many states also have statutes that require companies to **securely destroy SSN after no longer in use**.
			9. **California** prohibits businesses as well as state and local agencies from using SSN for **public posting**, printing **on mailings** (unless mandated by federal law), and printing on **ID or membership cards**. Also **prohibits businesses from requiring** consumers to **transmit SSN over unencrypted internet connection**.
		2. **Data destruction**: **At least 35 states have data destruction laws**, which are **sometimes incorporated into data breach laws.**
			1. **Common elements of State laws**:
				1. **Who it applies to** (government and/or private businesses)

any business that conducts business in the state and any business that maintains or otherwise possesses personal information of a resident of the state

entities must take “reasonable measures” to safeguard PI against unauthorized access in connection with or after its disposal

**subcontracting allowed after due diligence** (i.e., reviewing an independent audit of operations, references and requiring independent certification of the business or personally evaluating the competency and integrity of the disposal business)

**reasonable measures** are

**burning, pulverizing or shredding** so that PI cannot be practicably read or reconstructed

**destruction or erasure of electronic media and other non-paper media** so cannot be practicably read or reconstructed

description of procedures for adequate destruction or proper disposal of personal records as official **written policy of the business** entity

* + - * 1. **Requires notice**
				2. **Exemptions** (e.g., GLBA, HIPAA, CRAs subject to FCRA)
				3. **Covered media** (e.g., electronic and/or paper)
				4. **Penalties** – statutory damages, whether there’s a private right of action
			1. **Differences Among States**
				1. **AZ** applies **only** to **paper**
				2. **AK** authorized **private right of action**
				3. **NM** requires shredding, erasing **or otherwise modifying the PII** contained in records to make it unreadable or undecipherable
				4. **CA** requires destruction such that records are “unreadable or undecipherable through **any means**”
				5. **VA** applies **only to govt entities**
				6. **MA has steep penalties** of not more than $100 per data subject affected and up to $50K for each instance of improper disposal
		1. **Security procedures**:
			1. **Incident Mgmt for Data Breach**: Privacy pro must support and often lead efforts to **prevent, detect, contain and report security breaches**
				1. **Steps for Incident Management**

**Determine whether breach actually occurred**

**Evidence of breach** – multiple failed login attempts, sudden use of dormant access accounts, use of info systems after hours, presence of unknown programs, files, devices or users

**Containment, analysis** and **documentation** of the incident

**Notify** affected parties

Several **states** have **specific requirements** for **content of notification letter**

**Contractual** obligations to notify

**Timing** for notification – deadlines for notice upon discovery

Premature notice with inaccurate or incomplete facts can exacerbate the issue

**Implement effective follow-up** assessment and methods, such as additional training, internal self-assessments and third-party audits where needed – assess the breach as well as the incident response plan to identify deficiencies

* + - * 1. **Best Practices for Security Breach Plan**: 2017 Executive Office of President’s Office of Management and Budget (OMB) requirements for federal agencies preparing for and responding to PII security breaches:

**Designate** members who will make up the **breach response team**

**Identify** applicable privacy **compliance documentation**

**Share** **information about the breach** to understand its extent

**Determine** **reporting requirements**

**Assess risk of harm** for individuals potentially affected by breach

**Mitigate risk of harm** for individuals potentially affected by breach

**Notify individuals** potentially affected by the breach

* + - * 1. **OMB also requires Vendors** to be contractually required to do the following:

provide **training** to their employees on identifying and reporting a breach

properly **encrypt** PII,

**report** suspected or confirmed breaches

participate in the **exchange of information** in case of a breach,

**cooperate** in the investigation of a breach

**make staff available** to participate in breach response team

* + - 1. **Exceptions to Data Breach Notification**
				1. Entities subject to **more stringent** data breach notification laws
				2. Entities that **already follow** breach notification procedures as part of **their own information security policies** as long as these are **compatible with** the requirements of **state law**
				3. Whether a **safe harbor** exists for data that was **encrypted, redacted, unreadable or unusable**
		1. **Recent developments**
			1. **California Electronic Communications Privacy Act (2015)**: CalECPA affects any person or entity that receives California **warrant or order related to electronic communications**, including California and foreign corporations.
				1. **No California government entity can search phones and no police officer can search accounts without**:

Permission from a **judge**

Obtaining **consent**

Showing it is an **emergency**

* + - * 1. A **warrant** is **always required** to obtain **location information or IP addresses**
				2. **Warrant for electronic information** (both communications and device information) **requires**

**Description of information to be seized** by specifying:

The **time periods** covered

And, as appropriate and reasonable:

the **target** individuals or accounts,

the **applications or services** covered

the **information sought**

That information obtained through execution of warrant that is unrelated to objective of warrant is sealed and not subject to further review, use, or disclosure w/o court order

* + - * 1. **Voluntary disclosures to govt entity** still **allowed if** disclosure **not otherwise prohibited** by state or federal law
				2. **Targets and recipients** of legal process **both have standing to petition court** “to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.”
				3. **Shifting burden for user notice** - burden on **govt to contemporaneously notify the targets** of legal process when requesting their data unless order for delayed notice granted. **Does not prohibit service providers from independently notifying users when their data has been requested** under legal process if delayed notice order not in place.
			1. **Delaware Online Privacy and Protection Act (2016)**: DOPPA covers more subject matter than other privacy laws. **Main principles** include:
				1. **Prohibits online advertising to minors related to products these consumers are not legally permitted to buy** (i.e., alcohol, tobacco, firearms, dietary supplements and sexually explicit material) and also restricts certain online advertising practices based on the minors’ personal information.
				2. Delaware law defines a minor as a state **resident under the age of 18**.
				3. Also applies to websites not necessarily directed to minors, but also to **websites known to be frequented by minors**
				4. **Privacy policies must be conspicuously posted**
				5. Acknowledging that **3rd parties do not have a right to know viewing habits of e-book users without informed consent** absent special compelling circumstances, DOPPA **prohibits e-book services from disclosing PII of readers to 3rd parties unless certain exceptions apply**, such as law enforcement or by court order
			2. **Nevada SB 538 (2017)**:
				1. **Third state (behind California and Delaware) to regulate online collection and disclosure of PII and to specifically legislate the info that must be included in privacy policies**.
				2. Requires operators of websites and online services to provide **notice to Nevada residents of** their **practices regarding collection and disclosure of PII**.
				3. Operators must make notice available in a reasonably accessible manner that:

Identifies the **categories of collected info** and the categories of **3rd parties** with whom the operator may **share PII**

Describes any process for the consumer to review and request changes to his PII, if the operator has such a process

Describes the process by which consumers will be notified of any material changes to the notice

Discloses **whether a 3rd party may collect PII** when the consumer uses the internet website or online service; and

States the **effective date of the notice.**

* + - 1. **Illinois Right to Know Act (2017)**: Passed by State Senate and bill is in committee in the State House – **Failed to reach a vote**. Provides that an operator of a commercial website or online service that collects PII through the Internet about individual customers residing in Illinois who use or visit its commercial website or online service must notify customers of specified information pertaining to its personal information sharing practices. Notably, it proposed a private right of action for violations.
				1. **Illinois Geolocation Privacy Protection Act**: proposed protection for geolocation information collected from smartphone apps. Passed both state chambers and was **vetoed by governor**.
			2. **New Jersey Personal Information and Privacy Protection Act (2017)**: limits the purposes for which **retail establishments** can lawfully **scan a person’s govt-issued ID card**, such as a driver’s license. Also limits **data that can be collected from such scanning** and **how these data can be retained and used**.
				1. Can collect only name, address, birthdate, ID card number, and jurisdiction that issued the card
				2. Allowed to scan for **only 8 specified purposes** (verify identity/age, prevent fraud, establish/maintain contractual relationship, if required to comply with another law – HIPAA, GLBA, FCRA)
				3. If scanned for **identity/age** – data **cannot be retained**
				4. If scanned for **other list purposes** – must be **securely stored**
				5. **Cannot not “sell or disseminate to a third party** any information obtained” for any purpose
				6. **Penalties** – **fines** and **private right of action** against retailer
			3. **Biometric Data**
				1. **What is Biometric Data**: **unique identifying characteristics** of a person’s body or mind and is separated into two categories: **physiological** (DNA, retinal scans, fingerprints, shape of a person’s hand or face or the sound of their voice) and **behavioral** (a person’s specific movements and actions or thought patterns)
				2. **Arkansas**, **California**, **Washington** and **New York** **amended their existing state privacy laws** to include **biometric data in the definition of PI** and have extended existing protections to biometric data.
				3. **Washington Biometric Privacy Law (H.B. 1493) (2017)**: Washington was the 3rd state (after Illinois and Texas) to enact a law regulating biometric information. Prohibits any company or individual from entering biometric data into a database **without providing notice, gaining consent OR providing a mechanism for preventing subsequent use of the biometric data for a commercial purpose**.

Collecting biometric data w/o consent or notice is allowed if not entered into a database w/o means for preventing subsequent commercial use

**Enrollment** of a biometric identifier in a database **for a commercial purpose requires** (i) providing **notice**; (ii) obtaining **consen**t; **or** (iii) providing mechanism to **prevent subsequent use** of biometric identifier **for a commercial purpose**

**After enrolled** in database, entity **prohibited from selling, leasing or disclosing w/o consent**

**Biometric Identifier defined** as “data generated by **automatic measurements** of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual”

Definition of biometric identifier **expressly excludes** “physical or digital photograph, video or audio recording or data generated therefrom” and makes **no mention of** face geometry (seems to be avoiding facial recognition technology and related litigation)

**Flexible Notice & Consent**: exact notice and type of consent required for enrollment is “**context-dependent**” (similar to 2012 FTC Report) and that notice need only be provided in a way that is “reasonably designed to be readily available to affected individuals.”

**Exempts** the collection, capture, enrollment or storage of a **biometric identifier** **from the notice and consent requirement** if used in furtherance of a “**security purpose**.”

**No private right of action**.

Of the three biometric laws, the new **Washington law is the only one that exempts use of a biometric identifier for purposes of security or fraud prevention from notice and consent requirements**

* + - * 1. **Illinois Biometric Information Privacy Act of 2008 (BIPA)**: Illinois was 1st state to regulate collection, use and disclosure of biometric data. Many states have used BIPA as a model. BIPA requires

**Notice**: **publicly available written policy** that includes a **retention schedule** and guidelines for **permanently destroying** biometric information or identifiers **after initial purpose** for collecting/obtaining satisfied **or w/in 3 years** after individual’s **last interaction** w/entity (whichever occurs first)

**Notice & Consent**: **written statement** with **specific purpose and retention period for collection** or capture of any biometric information and **written release from individual**, with similar restriction on entity’s ability to disclose the information

**Private right of action** to sue for mere violation of the law’s requirements, **even if no actual injury –** Illinois SCt held individual **need not suffer harm for standing to sue** under BIPA

* + - * 1. **Texas Biometric Privacy Act of 2009 (Capture or Use of Biometric Identifier Act (CUBI))**: covers all organizations and prohibits capture biometric information for a **commercial purpose** unless individual is first **informed** and has **consented** to the data collection. Also limits sale or disclosure of biometric information except under limited circumstances.

**Biometric identifier**  means retina or iris scan, fingerprint, voiceprint, or recording of hand or face geometry

**Does not specify** how **notice** provided **or consent** obtained

**No Sale, Lease or other Disclosure** unless

subject **consents** to disclosure for **ID purposes** in event of **death or disappearance**

disclosure **completes financial transaction** requested or authorized by individual

disclosure **required or permitted** by a federal or state statute

disclosure made by or **to law enforcement agency** for **law enforcement purpose** in response to a **warrant**

**Destroy** the biometric identifier **within a reasonable time**, but **not later than 1st anniversary** of **expiration of the purpose** for collecting the identifier (e.g., end of employment)

Does not apply to voiceprint data retained by FI

**Violation** subject to **fine** of not more than $25K per violation (no cap per incident) and enforced by State AG. No private right of action.

* + - 1. **New York Dept of Financial Services (NYDFS) Cybersecurity Regulation (2017)**: requires covered FIs and financial services companies to develop and implement **effective cybersecurity program** by assessing cybersecurity risk and developing a plan to proactively address identified risks.
				1. **Who**: FIs and financial services companies with >10 employees, >$5M in gross annual revenue from New York operations in each of past 3 years, **and** > $10M in year-end total assets (exempt if don’t meet any of these 3 criteria)
				2. **Covered FIs** are state-chartered banks, credit unions, investment companies, licensed lenders, mortgage brokers, life insurance companies, private bankers, commercial banks, and savings and loan associates
				3. Covered FIs must develop a **cybersecurity policy**, including an **incident response plan** that includes **data** **breach notifications within 72 hours**, which **aligns with** **industry best practices and ISO 27001** standards and **covers**:

Information security

Access controls and identity management

Business continuity and disaster recovery planning

Capacity and performance planning

Security of information systems, operations and availability

Systems and network security

Systems and application development and quality assurance

Periodic risk assessments

* + - * 1. **Cybersecurity program** in place **must align with** **NIST Cybersecurity Framework** and include:

risk assessments

documentation of security policies

designation of a CISO

limitations on data retention

incident response plan

audit trails

* + - * 1. **CISOs must prepare annual report** that includes

organization's cybersecurity policies and procedures

cybersecurity risks

effectiveness of current cybersecurity measures

* + - * 1. Covered FIs must develop a **written policy for vendor risk management**
				2. Covered FIs must complete **annual certification** process that requires **board of directors** to review cybersecurity program and **provide Certification of Compliance** w/NYDFS Cybersecurity Regulation.
			1. **California Consumer Privacy Act (CCPA) (2018)**
				1. **Does not replace** CA’s existing data protection laws:

**California Online Privacy Protection Act (CalOPPA)**: 1st law in US to require websites, online services, and mobile applications that collect PII about CA consumers to display **privacy notices on their site**. Also requires those services to **disclose tracking and collection of PII** and **how handle “do not track” requests**.

**Privacy Rights for California Minors in the Digital World Act**: allows **children under 18** to **request removal of content** they have posted online, requires sites to notify minors of **right to erasure**, and **prohibits websites and apps from advertising certain items** including alcoholic beverages and firearms to minors

**Shine the Light law**: requires **businesses that disclose customer information for direct marketing** purposes to **notify** customers

* + - * 1. **Scope**: a business must protect certain consumer privacy rights with respect to the **collection, use and sharing of PI**. These rights include the **right to request disclosure** of a business’ data collection and sales practices, the **right to request specific PI** collected, the **right to have certain PI deleted**, the **right to request that PI not be sold** to third parties (if applicable), and the **right not to be discriminated against because of exercising these rights**

**Business** meansa **for-profit business** that

**collects** or has collected on its behalf **PI of CA residents**

determines the **purposes and means** of processing the PI

**does business in CA**

**AND** meets ***one*** of the following:

at least **$25 M** in annual gross revenues

buys, sells, shares or receives PI of at least **50,000 CA consumers, households or devices** per year

derives at least **50%** of annual revenue **from selling** PI of CA residents

**OR**

**controls or is controlled** by an entity that meets the above criteria and **shares common branding** with that entity

**Consumer** means a **natural person who is a CA resident** (not corporations or other legal entities)

**Personal Information**: information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, as well as inferences drawn from such information to create profiles that reflect preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes of the consumer.

**Examples**:

Real name, postal address, email address, Social Security number, driver’s license number, passport number

Internet protocol (IP) address

Characteristics of protected classifications under California or federal law (such as race, religion, disability, sexual orientation, and national origin)

Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies

Biometric information

Internet and network activity, including “browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement”

Geolocation information

Audio, electronic, visual, thermal, olfactory, or similar information

Professional or employment information and certain education information

CCPA **does not apply to de-identified information** used by a business; that is, it **cannot reasonably** identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

**Required measures for using de-identified information**:

Technical safeguards that prohibit re-identification of the consumer to whom the information may pertain

Business processes that specifically prohibit re-identification of information

Business processes to prevent inadvertent release of de-identified information

Business must not attempt to re-identify the information

**Sale**: **any disclosure of PI** to another business or 3rd party **in exchange for value of any kind**, monetary or otherwise. “Sale” **does NOT include**:

**Disclosures of PI directed by the consumer**, or where consumer intentionally interacts with 3rd party through the business, if 3rd party does not further sell the PI inconsistently with CCPA.

Data **shared with 3rd parties** in order **to implement consumer’s decision to opt out** from data sales.

Data shared with **vendors to provide services to the business**, i.e., **Service Providers** that have a **written contract** with the business **that prohibits** **retention, use** or **disclosure of PI** except to provide services to the business

**Third Party that is not a Service Provider** may not sell PI that has been sold to the 3rd party by business unless consumer received express notice and opportunity to opt out of further sale

* + - * 1. **Notice**: Key requirements:

**Initial notice**. Business **must “at or before the point of collection,”** inform consumers regarding **categories of PI collected and purposes for use**. Collection includes direct and indirect collection of PI through any means, including “buying, renting, gathering, obtaining, receiving or accessing” the PI.

**Website notice**. As part of online privacy policy or any CA-specific description of rights, business **must describe consumer rights under CCPA**. If does not maintain online privacy notice or CA-specific description of rights, must post a description of these rights on its website. Notice must be **updated every 12 months**.

**“Right to opt out” notice**. Businesses that sell consumer PI must provide **“clear and conspicuous” link** on web site homepage that states, **“Do Not Sell My Personal Information.”** Description of right to opt out of data sales must also be provided in online privacy policies, if maintained by the business. After consumer exercises right to opt out, business must stop selling that consumer’s PI.

* + - * 1. **Individual Rights Regarding Personal Information**

**Right to Know** about PI a business collects about them and how used and shared

Categories of PI collected

Specific pieces of PI collected

Categories of sources from which the business collected PI

Purposes for which the business uses the PI

Categories of 3rd parties with whom the business shares the PI

Categories of information that the business sells or discloses to 3rd parties

**Right to Delete** PI collected and to tell Service Providers to do the same, subject to following **exceptions,** if maintaining the PI is required:

To **complete a transaction** or provide a service requested by the consumer, or complete or perform a contract between the business or consumer

Detect, protect against, or prosecute **security incidents or illegal activity**

For **debugging/repair** purposes

To **exercise legal rights**, including free speech rights **or** to **comply with legal obligations**

To engage in **research in the public interest**, where the consumer has provided **informed consent**

For **limited internal purposes** “**compatible with the context**” in which PI provided by consumer, **or reasonably aligned with consumer expectations**

**Right to Opt-Out** of the sale of PI. Businesses **must wait** **at least 12 months** before asking to opt back into sale of PI

**Right to Non-Discrimination** for exercising CCPA rights.

Business **cannot deny goods or services, charge a different price, or provide different level or quality of goods or services** because rights under CCPA exercised.

Businesses **can offer you promotions, discounts and other deals in exchange for collecting, keeping, or selling your personal information**. But **only if financial incentive offered is reasonably related to value of the PI**.

* + - * 1. **Data Breach**: To be entitled to enforcement and remedies, a data breach must consist of:

**unauthoriz****ed access and exfiltration, theft, or disclosure** of consumer’s PI due to

business’s **failure to implement and maintain reasonable security procedures and practices**

**Remedies do not apply to PI that is encrypted or redacted**. Remedies **only apply to** certain subset of **sensitive PI** (such as govt ID #s) and are not available for all categories of PI.

**Before action for damages**, must provide business **30 days’ advance written notice and opportunity to cure** alleged violation.

* + - * 1. **Enforcement**

Enforced by **CA AG** with 30-day cure period

**Civil penalties** between $2500 and $7500 (higher for intentional violations).

**Private right of action** to recover **statutory damages** of between $100 and $750 per individual per incident **or actual damages** (whichever greater) and **any other remedies deemed appropriate by a court**.

* + - 1. **Other significant state acts and laws**:
	1. **DATA BREACH NOTIFICATION LAWS (1-3 QUESTIONS)**

There is no federal data breach notification law. **All 50 states, D.C., Puerto Rico and the US Virgin Islands have state data breach notification laws, which create important incentives for companies to develop good info sec practices.** Other than MA, which has the most prescriptive state privacy laws and directly requires businesses to implement security controls, most state laws don’t require specific security controls but create an incentive for effective controls – reduced costs to the company of public disclosure of a breach.

* + 1. **Elements of state data breach notification laws**: state data breach notification laws contain same basic elements:
			1. **Definitions of relevant terms (personal information, security breach)**:
				1. Definition of **PERSONAL INFORMATION**, meaning the specific data elements that trigger reporting requirements

**CT is typical** (all states require this basic list): **first name or first initial and last name** combined **with at least one** of the following:

**SSN**

**State ID** (driver’s license number or state ID card number)

**Financial account number** or credit or debit card number **combined with** **security information** (security code, access code, or password) that permits access to the account

**Medical and Healthcare Information**: Alabama, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Virginia, and Wyoming

**Financial Account passwords, personal ID #, account #, etc**.: Alaska, Georgia, Maine, North Carolina, and Vermont

**Federal or State Govt ID #** (passport, military, tax): Alabama, Colorado, Delaware, Maryland, Montana, New Mexico, New York, North Carolina, Oregon, South Carolina, South Dakota, and Wyoming

**Biometric Data** (unique physical or digital **representation of biometric data**, such as fingerprint, retina or iris image or **biometric data**, such as digital measurements of fingerprints, voice print, retina or iris image, facial characteristics or hand geometry): Arkansas, California, Colorado, Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, New York, North Carolina, Oregon, Washington, Wisconsin, and Wyoming

**DNA profile**: Delaware and Wisconsin

**Tax Information and Work**-**Related Evaluations**: Puerto Rico

**Mother’s Maiden Name**: North Carolina and North Dakota

**CCPA**: real name, postal address, email address, Social Security number, driver’s license number, and passport number; internet protocol (IP) address; characteristics of protected classifications under California or federal law (such as race, religion, disability, sexual orientation, and national origin);“commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;” biometric information; internet and network activity, including “browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement;” geolocation information; “audio, electronic, visual, thermal, olfactory, or similar information;” and professional or employment information and certain education information; ***including*** “**inferences drawn**” **from the above** data elements **to create profiles** that reflect “preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes” of the consumer

**All states** include **unencrypted data** and **computerized data**

**Data in any form, including written records**: Alaska, Hawaii, Iowa, Massachusetts, North Carolina, South Carolina, Washington, and Wisconsin

**Almost all states exclude publicly available information *except*** Michigan

**Ohio** has extremely **expansive** view of **exception** for publicly available information

* + - * 1. Definition of **COVERED ENTITIES**

**CT**: any ***person* who** **conducts business in this state**, and who, in the ordinary course of such person’s business, **owns, licenses or maintains** **computerized data** **that includes PI**

Some states limit this to ***entities that conduct business*** in the state

Some states are even narrower – **Georgia** applies **only to “information brokers”**

**CCPA**: a **for-profit business** that

**collects** or has collected on its behalf **PI of CA residents**

determines the **purposes and means** of processing the PI

**does business in CA**

**AND** meets ***one*** of the following:

at least **$25 M** in annual gross revenues

buys, sells, shares or receives PI of at least **50,000 CA consumers, households or devices** per year

derives at least **50%** of annual revenue **from selling** PI of CA residents

**OR**

**controls or is controlled** by an entity that meets the above criteria and **shares common branding** with that entity

* + - * 1. Definition of a “**SECURITY BREACH**” or “**breach of the security of a system**” **and level of harm** requiring notification

**CT**: unauthorized access to or acquisition of electronic files, media, databases or computerized data containing PI when access to the PI has not been secured by encryption or by any other method or technology that renders the PI unreadable or unusable

Some state require the **compromise** to be **“material”** (e.g., PA)

Several states define “breach” to be an event that causes or is likely to cause **identity theft or other material harm** (e.g., KS, SC)

**CCPA**: unauthorized access and exfiltration, theft, or disclosure of PI resulting from failure to implement and maintain reasonable security procedures and practices

* + - 1. **Conditions for notification (who, when, how)**:
1. **Whom to notify**:

**Affected state residents** (i.e., at risk because PI has (potentially) been exposed based on the level of unauthorized access or harm)

⅔ of states require **notification to State AG or other state agencies**

⅔ of states require **notification of nationwide CRAs**

**All states require 3rd party notification**

**CT**: Any person that maintains computerized data that includes PI that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the PI was, or is reasonably believed to have been accessed by an unauthorized person

1. **When to notify** affected parties: most common phrase used in conjunction with timing is “the **most expedient time possible and without unreasonable delay**”
* Most common time limit is w/in 45 days after discovery of the breach
* For companies operating nationally, best practice is to report w/in 30 days after discovery, meaning that a delay of 45 days could be considered unreasonable w/o explanation in some states
* Where breach is suspected to be result of criminal activity, most states allow delays for “reasonable period of time if LE agency determines that notification will impede the investigation *and* the LE agency has made a request that the notification be delayed”
* Puerto Rico: requires notification to Dept of Consumer Affairs w/in 10 days and Dept makes breach public w/in 24 hours (shortest period for required public disclosure in US)
1. **What to include** in the **notification letter** to affected parties

**States that specify contents of notification letter to state residents**: Alabama, California, Colorado, Delaware, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, Montana, New Hampshire, New Mexico, New York, North Carolina, Oregon, Rhode Island, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming (almost 50%)

**North Carolina** requirements among **most extensive**

**Oregon** requires **advice** to consumer to **report suspected identity theft to law enforcement**

**Massachusetts** and **West Virginia** **require** notification to **specify** **how to obtain police report** and **request credit freeze**

MA **prohibits** including **description of nature of the breach** in the notification or the **number of residents affected** by the breach

1. **How to notify** affected parties: states typically provide notification options but **written notice** to affected party is **always required first**. **Phone and email** are typical **alternatives** but usually only if **affected party** has previously **explicitly selected** one of these **as preferred communication method**

**CT**: **Substitute notice** shall consist of the following: (1) **Electronic mail** notice when the person, business or agency has an electronic mail address for the affected persons; (2) **conspicuous posting** of the notice on the **website** of the person, business or agency if the person maintains one; and (3) notification to **major state-wide media**, including newspapers, radio and television

1. **Notice requirements to state AG or state agency**: approx. **⅔ of states require notification** to State AG or other state agencies

**Timing of notice** **varies** but typically ASAP

Many states contain **no specific timing of notice to State AG** - California, Maine, New Hampshire, New York, and South Dakota

Many states have **threshold number of affected residents before notice** to State AG required (250, 500, 1000)

Most states require notification to State AG only if entity determines, after investigation into the breach, that the breach harmed or is reasonably likely to harm consumers

**Notice to State AG and regulators** may be sent **by letter or email**.

Some states have **online form that must be used** for this reporting (e.g., California, New York, North Carolina)

1. **When notice** is required to **CRAs**: approx. **⅔ of states** **require notification** to **nationwide CRAs**. CRAs have **established email addresses** to receive breach notifications.

Majority of these require notification of CRAs **if more than 1000 state residents** affected

**ME and NH** must notify if **more than 1000 consumers** are affected – regardless of residency

**MN and RI** must notify if **more than 500 residents**

**NY** must notify if **more than 5K residents**

**Georgia** – **information brokers** must notify CRAs if **more than 10K** GA residents

**TX** must notify if **more than 10K individual**s affected (regardless of residency)

**Montana** requires entities to **coordinate notification with CRAs**

1. **Exceptions** to obligation to notify (or when notification may be delayed)

**Most Common**: **Entity is subject to another more stringent data breach notification law**, such as HIPAA or the GLBA Safeguards Rule

**Internal Info Sec Policy**: most states allow exceptions for entities that already follow breach notification procedures as part of their own information security policies as long as these are compatible with the requirements of the state law

**Safe Harbor**: most states have a safe harbor for **data that was** **encrypted, redacted, unreadable or unusable** though specific requirements vary by state – some states exclude encrypted data from definition of breach or definition of PI or there’s no risk of harm. Encryption exception typically applies only when key remains secure. Most states make this explicit by stating that the exception does not apply when decryption key breached along with encrypted data. Some states contain more **technology-neutral language** than “encryption” and state that notification requirements do not apply when there is **no “reasonable likelihood of harm”** to affected persons after reasonable investigation, or similar language. If data is effectively encrypted, a breach did not “**compromise the confidentiality, security and integrity**” of the PI, which would not be a breach under laws with this “compromise” standard.

 ***CT is the only state that does not have this compromise language***

* + - 1. **Subject rights (credit monitoring, private right of action)**:
				1. **Penalties** and **private rights of action**

**Enforcement** generally reserved to the **State AG**

Many states **specify** **civil penalties**

**Private Right of Action** allowed by individuals **harmed by disclosure** of PI: Alaska, California, the District of Columbia, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, South Carolina, Tennessee, Virginia and Washington

**CCPA is 1st US law to allow recovery of statutory damages** as a results of a data security incident – consumers may be entitled to remedies including (1) statutory damages of between $100 and $750 per consumer, per incident or actual damages, whichever is greater; (2) injunctive or declaratory relief; and (3) any other relief deemed appropriate by the court. **NOTE**: these remedies are **not available for all categories of PI**, **only** available for a **certain subset of sensitive PI** (i.e., First Name or First Initial + Last Name + any one of SSN, # of govt issued ID or document, financial acct # + security access info, medical info, health insurance info or unique biometric data generated from measurements or technical analysis of human body characteristics). **That is**, these remedies are **NOT available for** breach of **username or email address** in combination **with password or security question and answer** that would permit access to online account

* + 1. **Key differences among states today**:
			1. Most states **exclude publicly available information** (typically info in public govt records) from definition of PI **except MI**
			2. ***2010 MA Personal Information Protection Regulation***: prescriptive encryption rule - all parties that “own or license” PI of MA residents **must encrypt all PI stored on laptops or other portable devices**, as well as **wireless transmissions** and **transmissions sent over public networks**
		2. **Recent developments**
			1. **Tennessee SB 2005 (2016, amended 2017)**:
				1. **2016**: **removed exemption for encrypted data** from its data breach notification provision – made TN **1st state in US** to **require breach notification regardless** of whether information subject to the breach was **encrypted**
				2. **2017 amendment**: **clarified** that **encrypted data** receives protection of the **safe harbor**, ***unless*** the **encryption key also acquired** in the breach
				3. Amendment also specified that an “**unauthorized person**” includes an **employee** **of the information holder** who is discovered to have **obtained personal information and** **intentionally used it for illegal purpose**.
				4. Requires **notice of breach** within **45 days after discovery** of the breach (absent a delay request from law enforcement), regardless of whether information was encrypted or not
			2. **California AB 2828 (2016)**: requires **data breach notifications** to be sent to residents when **encrypted PI** has been breached **and encryption** **keys or security credentials** **were**, **or** were **reasonably believed to have been, compromised** and could render the breached information readable or useable
			3. **Illinois HB 1260**:
				1. expanded definition of PI to include **health records, biometric data,** **usernames and email address when combined with** **password** or other information (e.g., security question and answer) that would allow **access** **to** an individual’s **online account**.
				2. Companies must **notify** individuals **by email or postal mail** **to change** their **credentials** (username, password or other identifiers such as a security question) if some combination of their username, password or other security information has been breached by a third party.
				3. Requires **notification of State AG for HIPAA data breaches**.
				4. Companies also required to take **reasonable security measures** **to protect records** from unauthorized breach, destruction or disclosure
				5. **Removed encryption safe harbor if decryption key was compromised**
				6. **CA, FL, WY, NB, NV** have **similarly amended definition of PI** subject to notification
			4. **New Mexico HB 15 (2017)**:
				1. **Definition of “PII”** 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 individual’s identity when individual accesses physical location, device, system or account.”
				2. **Applies to** **unencrypted computerized data** or **encrypted computerized data when encryption key** or code also **compromised**.
				3. Notice to **State AG and major CRAs** required if **more than 1,000 NM residents** are notified.
				4. **Notice** must be made to **NM residents** (and State AG and CRAs if over 1,000 residents are notified) **w/in 45** calendar days **of discovery** of security breach.
				5. **Third-party service providers** also required to notify data owner or licensor w/in 45 days of discovery of data breach
			5. **Massachusetts HB 4806**: amends certain provisions of the state data breach notification law, increasing reporting requirements on a person or agency collecting personal information of Massachusetts residents. **Expands notification requirements**, requires companies to contract with a third party to offer affected residents **free credit monitoring** **services**, and **prohibits security freeze fees**.
				1. **Notice to State Regulators must include**: (original in gray, amendments in black)

**Nature of the breach** of security

**Number** of residents affected

Steps person or agency intends to take regarding the breach of security

Name and title of the person or agency that experienced the breach of security;

Type of person or agency reporting the breach of security;

The **person responsible** for the breach of security, **if known**;

**Type of PI** compromised, including, but not limited to, social security number, driver’s license number, financial account number, credit or debit card number or other data;

Whether the person or agency maintains a written information security program; and

**Steps** the person or agency **has taken or plans to take** relating to the incident, including updating the written information security program

* + - * 1. **Notice to affected residents must include**:

resident’s **right to obtain a police report**

**how resident may request security freeze** (i.e., credit freeze on credit report so new accounts can’t be opened) and necessary information to be provided when requesting security freeze

indicate there will be **no charge for a security freeze**

fees by CRAs to “freeze” or “thaw” credit files of affected residents are prohibited - affected residents are allowed to place, lift, or remove security freezes without charge

mitigation services to be provided pursuant to Massachusetts’ data breach notification laws (*i.e.*, **free credit monitoring services)**

**MA is 4th state** (after CA, CT, and DE) to require companies to contract with 3rd party to offer **free credit monitoring services for at least 18 months (42 months if company is a CRA) to residents involved in security breach compromising SSNs**

Affected residents **cannot be required to waive right of action as condition to receiving credit monitoring services**

* + - * 1. **Slight Modification to Timing Requirements**: Existing timing obligations, which required companies to provide notification **as soon “as practicable and without unreasonable delay**,” remained **unchanged** **but** companies are **now prohibited from delaying notice** because **total number** of affected residents has **not yet been ascertained**.
			1. **Other significant state amendments**:

**The following represents updated content for 2020:**

• Data subject rights

• Privacy issues in artificial intelligence

• The Existing Business Relationship exception

• Federal preemption

• CCPA private right of action

• Data broker laws

• Restrictions on background checks

• Biometrics law