Grading on a Curve:

Privacy Legislation in the 116th Congress (2019-2020)

Electronic Privacy Information Center (EPIC)
Washington, DC

September 2019

EXECUTIVE SUMMARY

The United States is now considering several bills to protect privacy. These bills are intended to address growing public concern about the absence of adequate legal protection in the United States for personal data. EPIC's report **Grading on a Curve** reviews recent developments, identifies key characteristics of privacy laws, and assesses pending legislative proposals. The EPIC Report finds that all of the bills lack the basic elements of a comprehensive privacy law, such as a federal baseline for privacy protection, an opportunity for individuals to enforce their rights, and an independent data protection agency. However, Senator Ed Markey's (D-MA) **Privacy Bill of Rights Act**, S. 1214, is comprehensive and responds directly to many of the current privacy threats Americans face. EPIC ranks the **Privacy Bill of Rights Act** as the #1 bill in Congress.

A survey of privacy legislation in the 116th Congress also reveals that many bills have been referred to the Senate Commerce Committee, but the Committee has yet to schedule a public hearing on any of the legislative proposals. The House Energy & Commerce Committee has also not yet scheduled hearings on legislative proposals. Congress will need to hold hearings, invite experts, and seek comments from the public before acting on these proposals.

GROWING SUPPORT FOR PRIVACY LEGISLATION

There are many factors that have contributed to the growing support for privacy legislation in the United States Congress. These factors include:

Increase in data breach and identity theft. Identity theft is one of the top consumer complaints and the problem is getting worse. According the Federal Trade Commission, identity theft reports increased 15% from 2017 to 2018.[1] The cost of data breaches to the U.S. economy is substantial. Cybercriminals exposed 2.8 billion consumer data records in 2018, costing over $654 billion to U.S. organizations, according to ForgeRock.[2] "Personally identifiable information (PII) was the most targeted data for breaches in 2018, comprising 97% of all breaches."[3] Data breaches, though prevalent, are not inevitable; reasonable data security measures can prevent many of the most common forms of criminal hacking. But until data breach victims can hold companies legally accountable for their lax security, data breaches will continue to occur at an alarming pace.

Technology outpacing the law. There have been few updates to U.S. privacy law in almost two decades. In the 1980s, the United States enacted subscriber privacy provisions in the Cable Act,[4] the Electronic Communications Privacy Act,[5] and the Video Privacy Protection Act.[6] In the 1990s, the United States enacted the

Children's Online Privacy Protection Act,[7] the Health Insurance Portability and Accountability Act,[8] and the Telephone Consumer Protection Act.[9] The Fair and Accurate Transaction Act of 2003 gave consumers the right to obtain free credit reports.[10] But there have been no significant updates to U.S. privacy laws since then. Many other countries, including U.S. trading partners, have modernized their privacy laws in response to changes in technology and business practices. U.S. privacy law is considered out of date and ineffective.

Trade with Europe and the GDPR. US-based Internet firms collect and use the personal data of individuals outside of the United States, including many Europeans. Because the United States lacks a comprehensive privacy law and a data protection agency, European governments have expressed concern about privacy protection in the United States.[11] Under the Privacy Shield, the United States must show adequate protection for the personal data of Europeans,[12] but many key provisions of the agreement have been ignored.[13] U.S. companies have pledged support for the EU General Data Protection Regulation, but it remains unclear in practice whether U.S. companies will comply.

Public Support for Privacy Legislation. Opinion polls show widespread public support for stronger privacy protection in the United States.[14] In a 2018 poll by Pew Research, two-thirds of Americans said current laws are not good enough in protecting people's privacy, and 64% support more regulation of advertisers.[15] An earlier poll found there is broad support in the US for new legal protection for personal information.[16] Americans favor limits on how long the records of their activity are stored. According to Pew, 74% of Americans say it is "very important" to be in control of their personal information.

The Failure of the Federal Trade Commission. Unlike most democratic countries in the world, the United States does not have a data protection agency. For many years, the Federal Trade Commission held itself out as the privacy agency for the United States, and there were significant judgements against Internet firms, including Facebook,[17] Google,[18] and Microsoft.[19] But over time it became clear that the FTC lacked the authority, competence, and political will to safeguard American consumers. The recent settlements with Facebook and Google, though record-setting, have been widely criticized.[20] There is little change in the companies' business practices and no compensation for those whose personal data was exploited.

California Consumer Privacy Act. In 2019, California enacted the California Consumer Privacy Act, important privacy legislation that established new safeguards for users of Internet-based services.[21] Many other states, including Hawaii, Massachusetts, and Illinois, are considering enactment of similar laws, continuing a long tradition of state-based privacy protections.[22] The action at the state level has raised obvious questions about why Congress has not done more to safeguard privacy in the United States.

ELEMENTS OF A PRIVACY LAW

The key elements for privacy legislation identified in EPIC's Report **Grading on a Curve** follow from commonly recognized national and international standards for data protection. For example, the OECD Privacy Guidelines of 1980 are widely viewed as a baseline standards for privacy rights and responsibilities and have been adopted in U.S. law and international agreements.[23] More recently, the General Data Protection Regulation of the European Union has emerged as the most comprehensive approach to privacy protection in the modern age.[24] The modernized Council of Europe Privacy Convention has also shaped the modern day understanding of the right to privacy.[25]

Strong definition of personal data

> *"The term 'personal information' means information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to, a particular individual."*
>
> *- S.1214 (Sen. Markey)*

The scope of a privacy bill is largely determined by the definition of personally identifiable information or "personal data," in the terminology of the GDPR. A good definition recognizes that personal data includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. A good definition of personal data will typically include a non-exclusive list of examples. Personal data also includes all information about an individual, including information that may be publicly available, such as zip code, age, gender, and race. All of these data elements are part of the profiles companies create and provide the basis for decision-making about the individual. So, bills that exclude publicly available information misunderstand the purpose of a privacy law.

Establishes an Independent Data Protection Agency

Almost every democratic country in the world has an independent federal data protection agency, with the competence, authority, and resources to help ensure the protection of personal data. These agencies act as an ombudsman for the public. The United States has tried for many years to create agencies that mimic a privacy agency, such as the Privacy and Civil Liberties Oversight Board, or to place responsibilities at the Federal Trade Commission. Many now believe that the failure to establish a data protection agency in the United States has contributed to the growing incidents of data breach and identity theft. There is also reason to believe that the absence of a U.S. data protection agency could lead to the suspension of transborder data flows following recent decisions of the Court of Justice of the European Union.[26]

Individual rights (right to access, control, delete)

The purpose of privacy legislation is to give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals exercise against companies that choose to collect and use their personal data. These rights typically include the right to access and correct data, to limit its use, to ensure it is security protected, and also that it is deleted when no longer needed. "Notice and consent," although it appears in several of the proposed bills, has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual.

> *"Each agency that maintains a system of records shall, upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system."*
> *- Privacy Act of 1974, 5 U.S.C. § 552a(d)*

Strong data controller obligations

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as "Fair Information Practices." Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/Disclosure limitations
- Data minimization and deletion
- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

Algorithmic Transparency Requirements

> *"AI Actors should [...] enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."*
> *- OECD AI Guidelines (2019)*

As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms. All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability. For example both the GDPR and the Council of Europe Privacy Convention—new laws that address emerging privacy challenges—have specific articles to ensure accountability for algorithmic-based decision-making.

Data Minimization and Privacy Innovation Requirements

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.

> *"[Covered entities must] take reasonable measures to limit the collection, processing, storage, and disclosure of covered data to the amount that is necessary to carry out the purposes for which the data is collected; and store covered data only as long as is reasonably necessary to carry out the purposes for which the data was collected."*
> *- S.584 (Sen. Cortez Masto)*

Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data.

Prohibits take-it-or-leave-it or pay-for-privacy terms

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

Private Right of Action

> *"Any individual alleging a violation of this Act or a regulation promulgated under this Act may bring a civil action in any court of competent jurisdiction."*
> *- S.1214 (Sen. Markey)*

Privacy laws in the United States typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called "liquidated" or "stipulated" damages are a key element of US privacy law and should provide a direct benefit to those whose privacy rights are violated. Several of the bills pending in Congress rely on the Federal Trade Commission to enforce privacy rights, but the FTC is ineffective. The agency ignores most complaints it receives, does not impose fines on companies that violate privacy, and is unwilling to impose meaningful penalties on repeat offenders.[27]

Limits Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[28]

> *"Personal information may only be disclosed to a law enforcement agency, "pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent state warrant, a grand jury subpoena, or a court order."*
>
> *- Video Privacy Protection Act*

Does Not Preempt Stronger State Laws

> *"Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy."*
>
> *- Cable Communications Privacy Act*

A well-established principle in the United States is that federal privacy law should operate as a floor and not a celling. That means that Congress often passes privacy legislation that sets a minimum standard, or "baseline," for the country and allows individual states to develop new and innovative approaches to privacy protection. The consequences of federal preemption are potentially severe and could include both a reduction in privacy protection for many consumers, particularly in California, and also a prohibition on state legislatures addressing new challenges as they emerge. That could leave consumers and businesses exposed to increasing levels of data breach and identity theft from criminal hackers and foreign adversaries.

THE LEGISLATIVE PROPOSALS

Bill	Markey	Cortez-Masto	Rubio	Klobuchar-Kennedy	Delbene	Blackburn
Strong definition of personal data	✓		✓		✓	✓
Establishes a Data Protection Agency						
Individual rights (right to access, control, delete)	✓	✓	✓			
Strong data controller obligations	✓	✓				
Algorithmic transparency requirements						
Data minimization & privacy innovation requirements	✓	✓				
Prohibits "take-it-or-leave-it" or "pay-for-privacy terms"	✓	✓				✓
Private right of action for consumers	✓					
Limits government access to personal data						
Does not preempt stronger state laws	✓	✓		✓		

Privacy Bill of Rights Act (S.1214)

Sen. Edward Markey [D-MA]

A-

Introduced: April 11, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.
EPIC Score: 48/100

"The Privacy Bill of Rights Act sets out a comprehensive approach to privacy protection."

Pros:

- Comprehensive approach, based on Fair Information Practices
- Establishes a private right of action so individuals can enforce their rights
- Important provisions on data minimization and deidentification
- Prohibits bias and discrimination in automated decision-making

Cons:

- No data protection agency
- Definition of personal data excludes publicly available information
- No limits on government access

DATA Privacy Act (S. 584)

Sen. Catherine Cortez Masto [D-NV]

B+

Introduced: February 27, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.
EPIC Score: 37/100

"A former state Attorney General, Sen. Cortez Masto goes beyond "notice and choice" by setting strong data security and privacy requirements, including data minimization and bans on practices that result in discrimination."

Pros:

- Bans discriminatory ad targeting
- Strong data minimization requirements

- Strong individual rights (right to access, control, delete)
- Required data security practices for data controllers

Cons:

- No private right of action
- No data protection agency
- No limits on government access

American Data Dissemination Act (S. 142)

B

Sen. Marco Rubio [R-FL]

Introduced: January 16, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.
EPIC Score: 27/100 (if Privacy Act of 1974 provisions are adopted)

"Fails to deliver on its Privacy Act promise and with a cumbersome mechanism for enactment."

Pros:

- Based on the Privacy Act of 1974[29], an excellent framework for privacy legislation
- Should include strong privacy rights and obligations, if following the Privacy Act framework

Cons:

- Delays implementation with FTC rulemaking
- Preempts stronger state laws
- No data protection agency (though original Privacy Act did include DPA)

Social Media Protection and Consumer Rights Act (S. 189)

B-

Sen. Amy Klobuchar [D-MN]
Sen. John Kennedy [R-LA]

Introduced: January 17, 2019
Status: Referred to Senate Commerce Committee. No hearing scheduled.
Co-sponsors: Sen. Richard Burr [R-NC], Sen. Joe Manchin III [D-WV]
EPIC Score: 19/100

"The Social Media Privacy and Consumer Rights Act is based on the ineffective 'notice and choice' model, but does create an important 72-hour breach notification standard."

Pros:

- Requires affirmative consent before instituting a material change that overrides a user's privacy settings
- 72-hour breach notification
- Right of access
- Strong authorities for state attorneys general

Cons:

- Narrow definition of personal data – only information collected online.
- Limited individual rights
- Minimal obligations on data controllers
- No restrictions on algorithmic decision making

Information Transparency & Personal Data Control Act (H. R. 2013)

C

Rep. Susan K. Delbene [D-WA-1]
Rep. Kathleen M. Rice [D-NY-4]
Rep. Thomas R. Suozzi [D-NY-3]

Introduced: April 1, 2019
Status: Referred to the House Committee on Energy and Commerce. No hearing scheduled.

Co-Sponsors: Rep. Ed Case [D-HI-1] , Rep. Alcee Hastings [D-FL-20], Rep. Matt Cartwright [D-PA-8], Rep. Steven Horsford [D-NV-4], Rep. Elissa Slotkin [D-MI-8], Rep. Seth Moulton [D-MA-6], Rep. Earl Blumenauer [D-OR-3], Rep. Tulsi Gabbard [D-HI-2], Rep. John Larson [D-CT-1], Rep. Donald Beyer, [D-VA-8], Rep. Abigail Davis Spanberger [D-VA-7], Rep. Rick Larsen [D-WA-2], Rep. Tim Ryan [D-OH-13], Rep. Kim Schrier [D-WA-8], Rep. Chrissy Houlahan [D-PA-6], Rep. James Himes [D-CT-4], Rep. Charlie Crist [D-FL-13], Rep. Denny Heck [D-WA-10], Rep. William Keating [D-MA-9], Rep. Derek Kilmer [D-WA-6]

EPIC Score: 10/100

"The Data Control Act provides few protections for individuals while prohibiting states from passing stronger protections."

Pros:

- Strong definition of personal data: "information relating to an identified or identifiable individual"
- Gives power to State Attorneys General to enforce the Act

Cons:

- Based on "notice and choice"
- Broad exemptions from the Act's requirements
- Requires privacy audits by third parties, but does not require that those audits be made public
- Preempts stronger state laws

Balancing the Rights Of Web Surfers Equally and Responsibly (BROWSER) Act (S. 1116)

F

Sen. Marsha Blackburn [R-TN]

Introduced: April 10, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.
Co-sponsors: Sen Tammy Duckworth [D-IL], Sen. Martha McSally [R-AZ]
EPIC Score -4/100

"The Browser Act favors industry groups over American consumers. The Act would also prevent states from passing stronger laws."

Pros:

- Good definition of personal data: "is linked or reasonably linkable to an individual."
- Prohibits "pay for privacy" provisions or "take it or leave it" terms of service

Cons:

- Based on "notice and choice"
- Contains no rulemaking authority
- Weak enforcement provisions
- Preempts stronger state laws

RELATED LEGISLATION

Data Accountability and Trust Act (H.R.1282)
Representative Bobby Rush [D-IL-1]

Introduced: February 15, 2019
Status: Referred to the House Subcommittee on Consumer Protection and Commerce. No hearing scheduled.

Requires the Federal Trade Commission to issue regulations requiring data controllers to establish security policies. Requires notification of breaches with 30 days.

A bill to amend the Children's Online Privacy Protection Act of 1998 (S. 748)
Senator Edward Markey [D-MA]
Senator Josh Hawley [R-MO]

Introduced: March 12, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.

Bans targeted advertising directed at children. Prohibits internet companies from collecting personal and location information from anyone under 13 without parental consent, and from anyone 13 to 15 years old without the user's consent. Revises COPPA's "actual knowledge" standard to a "constructive knowledge" standard for the definition of covered operators. Requires online companies to explain the types of personal information collected, how that information is used and disclosed, and the policies for collection of personal information. Prohibits the sale of internet connected devices targeted towards children and minors unless they meet robust cyber security standards. Requires manufacturers of connected devices targeted to children and minors to prominently display on their packaging a privacy dashboard detailing how sensitive information is collected, transmitted, retained, used, and protected.

Clean Slate for Kids Online Act (S. 783)
Senator Richard Durbin [D-IL]
Senator Edward Markey [D-MA]

Introduced: March 13, 2019
Status: Referred to Senate Commerce Committee. No hearing scheduled.

Gives individuals the right to have website operators delete information collected for or about them while they were under 13 years old, even if a parent consented to the collection.

Commercial Facial Recognition Privacy Act of 2019 (S. 847)
Senator Roy Blunt [R-MO]
Senator Brian Schatz [D-HI]

Introduced: March 14, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.

Requires companies to obtain the affirmative consent of the end user before using facial recognition technology to identify or track an end user.

Deceptive Experiences To Online Users Reduction (DETOUR) Act (S. 1084)
Senator Mark Warner [D-VA]
Senator Deb Fischer [R-NE]

Introduced: April 9, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.

Prohibits segmenting consumers for the purposes of behavioral experiments, unless with a consumer's informed consent. Requires large online operators to create an internal Independent Review Board to provide oversight on these practices. Prohibits user design intended to create compulsive usage among children under the age of 13 years old. Enables the creation of a self-regulatory professional standards body, to focus on best practices surrounding user design for large online operators.

Genetic Information Privacy Act of 2019 (H.R.2155)
Representative Bobby Rush [D-IL-1]

Introduced: April 9, 2019
Status: Referred to the House Energy and Commerce Committee. No hearing scheduled.

Requires genetic testing services to obtain express consent for disclosure of personally identifiable information or informed consent for the use or disclosure of PII for medical research. Enforced by the Federal Trade Commission and State Attorneys General. Preempts state laws.

Algorithmic Accountability Act of 2019 (S. 1108/H.R.2231)
Senator Ron Wyden [D-OR]
Senator Cory Booker [D-NJ]
Representative Yvette Clark [D-NY-9]

Introduced: April 10, 2019
Status: S. 1108: Referred to the Senate Commerce Committee. No hearing scheduled.
H.R. 2231: Referred to the House Energy and Commerce Committee. No hearing scheduled.

Directs the Federal Trade Commission to require large data controllers and processors to conduct impact assessments to determine if their algorithms are "inaccurate, unfair, biased, or discriminatory."

Data Breach Prevention and Compensation Act of 2019 (S.1336/H.R. 2545)
Senator Elizabeth Warren [D-MA]
Senator Mark Warner [D-VA]
Rep. Elijah Cummings [D-MD-7]

Introduced: May 7, 2019
Status: S.1336: Referred to the Senate Banking Committee. No hearing scheduled.
H.R. 2545: Referred to the House Financial Services Committee. No hearing scheduled.

Establishes an Office of Cybersecurity at the Federal Trade Commission, tasked with annual inspections and supervision of cybersecurity at credit reporting agencies. The FTC would impose mandatory, strict liability penalties for breaches of consumer data beginning with a base penalty of $100 for each consumer who had one piece of personal identifying information (PII) compromised and another $50 for each additional PII compromised per consumer. Fifty percent of the penalty must be used to compensate consumers.

Do Not Track Act (S.1578)
Senator Josh Hawley [R-MO]
Senator Mark Warner [D-VA]

Introduced: May 21, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.

Similar to the "Do Not Call" list, the Do Not Track Act would give individuals the ability to tell online companies that they do not want their data collected and targeted advertising directed at them. The Act is enforced by the FTC.

Protecting Personal Health Data Act (S.1842)
Senator Amy Klobuchar [D-MN]
Senator Lisa Murkowski [R-AK]

Introduced: June 13, 2019
Status: Referred to the Senate Health, Education, Labor, and Pensions Committee. No hearing scheduled.

Requires the Secretary of Health and Human Services to issue rules for new health technologies such as health apps, wearable devices, and genetic testing kits that are not regulated under HIPAA. The rules must limit the collection, use, and disclosure of personal health data.

Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data (DASHBOARD Act) (S.1951)
Senator Mark Warner [D-VA]
Senator Josh Hawley [R-MO]

Introduced: June 25, 2019
Status: Referred to the Senate Banking Committee. No hearing scheduled.

Requires large data controllers and processors (services with over 100 million monthly active users) to disclose to users what type of data is collected and provide users with an assessment of the value of that data.

Data Broker List Act of 2019 (S.2342)
Senator Gary Peters [D-MI]
Senator Martha McSally [R-AZ]

Introduced: July 30, 2019
Status: Referred to the Senate Commerce Committee. No hearing scheduled.

Requires data brokers to implement a comprehensive information security program and to register annually with the Federal Trade Commission.

GRADING CRITERIA

1. **Federal Baseline – States given room to innovate (15)**
    - Establishes federal baseline (10 points), or
    - No language on preemption (5), or
    - Explicit preemption of state law (-10 points)

2. **Definition of "personal data" (5)**
    - Information that identifies or could identify a particular person (3)
    - Information that allows an individual to be singled out for interaction, even without identification (Includes IP addresses and other similar identifiers) (1)
    - Data anonymization – when no collection of personal data is necessary for the legitimate purpose (1)

3. **Establishes Data Protection Agency (15)**
    - Establishes an independent data protection agency (10)
    - Rulemaking authority (2)
    - Enforcement powers (3)

4. **Enforcement (15)**
    - Private right of action (4)
    - State attorney general authority (3)
    - Stipulated damages (2)
    - Injunctive relief (2)
    - Statutory damages for violations of act (no requirement to prove negligence or prove actual damage) (4)

5. **Algorithmic transparency (5)**
    - Gives individuals the right to know the basis of an automated decision that concerns them (2)
    - Prohibits bias and discrimination in automated decision-making (2)
    - Requires independent accountability for automated decisions (1)

6. **Prohibits "take it or leave it" terms (3)**
    - Prohibits "pay-for-privacy" provisions or "take it or leave it" terms of service (1)
    - Requires meaningful, informed, and revocable consent (1)
    - Requires 'unbundling' of each required consent, and removal from consents of information for which consent is not required (1)

7. **Promotes Data Minimization and Privacy Innovation (7)**
    - Data minimization requirements (3)
    - Requires Privacy enhancing techniques (1)
    - Privacy by design an affirmative obligation (1)
    - Mandatory encryption (1)
    - Privacy settings by default to be the most privacy-protective options (1)

8. **Individual Rights (right to access, control, delete) (15)**
    - Confirmation of whether personal data is collected (3)
    - Obtain data about her in possession of controller (3)
    - Obtain information about who has access to data and how it used (2)
    - Challenge to denial of access (3)
    - Ability to have personal data (4)
        - Erased
        - Corrected
        - Completed
        - Amended

9. **Data Controller Obligations (15)**
    - Transparency about business practices (2)
        - Openness about developments, practices, and policies
        - Existence of data systems
        - Purpose of use of data
        - Identity and location of data controller
    - Data collection limitations (3)
        - Limits on collection - collection limited to what is necessary for legitimate purpose
        - Lawful collection
        - Fair collection
        - Knowledge or consent where appropriate
    - Use/disclosure Limitations (2)
        - Presumption against disclosure / new use inconsistent with purpose specification
        - Narrow exception for consent of data subject
        - Narrow exception for legal authority
        - Enhanced limits on the collection, use and disclosure of data of children and teens
    - Purpose specification (2)
        - Purpose stated
        - Purpose specified at time of collection

        - Subsequent use consistent with purpose
        - New purpose specified for new use
    - Accountability (2)
        - Data controller is specified
        - Compliance is required
        - Accountability mechanisms are established
    - Confidentiality/Security (2)
        - Protection against loss
        - Protection against unauthorized access
        - Protection against unauthorized destruction
        - Protection against unauthorized use
        - Protection against unauthorized modification
        - Protection against unauthorized disclosure
    - Data accuracy (2)
        - Data is relevant for purpose
        - Data is necessary for purpose
        - Data is accurate
        - Date is complete
        - Data is up-to-date

10. Limit government access to personal data (5)

- Requires a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order; (2)
- Requires clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; (1)
- Requires that law enforcement provide the individual concerned with prior notice and the opportunity to contest the search; (1)
- Authorizes the court reviewing the warrant application to modify the order if the scope of records requested is unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden. (1)

"FAIR INFORMATION PRACTICES" / OECD PRIVACY GUIDELINES

"Fair Information Practices" describe the rights and responsibilities associated with the collection and use of personal data. The most familiar articulation of Fair information Practices are the OECD Privacy Guidelines set out below. (The eight guidelines were first described in the 1977 report of the US Privacy Protection Study Commission which stated that they can be found in the US Privacy Act of 1974.[30]):

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance the stated purpose except:

a) with the consent of the data subject; or
b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the

main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
    1. within a reasonable time;
    2. at a charge, if any, that is not excessive;
    3. in a reasonable manner; and
    4. in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

REFERENCES

Cable Communications Policy Act of 1984.

California Consumer Protection Act of 2019 ("CCPA").

Children's Online Privacy Protection Act of 1998 ("COPPA")

Council of Europe, **Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (2018) ("COE Convention 108+")

Drivers Privacy Protection Act of 1994 ("DPPA")

Electronic Communication Privacy Act of 1986 ("ECPA")

European Union, **General Data Protection Regulation** (2016)

Fair and Accurate Credit Transactions Act of 2003 ("FACTA")

Gramm-Leach-Bliley Act ("GLBA")

Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

National Conference of State Legislatures, ***State Laws Related to Internet Privacy*** (2019)

National Telecommunications and Information Administration, *NTIA Seeks Comment on New Approach to Consumer Data Privacy* (Sept. 28, 2018)

OECD AI Principles (2019)

OECD Privacy Guidelines (2013)

Privacy Act of 1974

Privacy and Digital Rights for All, *A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019)

Marc Rotenberg, *The Privacy Law Sourcebook* (EPIC 2018)

Telephone Consumer Protection Act of 1991 ("TCPA")

Video Privacy Protection Act of 1988 ("VPPA")

GLOSSARY

Algorithm
Complex mathematical formulas and procedures implemented into computers that process information and solve tasks.[31]

Anonymization
A process by which identifying information is removed from a data set. After data anonymization, it should be impossible to learn the individual's identity associated with the data set.

In order to protect the privacy interests of consumers, personal identifiers, such as name and social security number, are often removed from databases containing sensitive information. This anonymized, or de-identified, data safeguards the privacy of consumers while still making useful information available to marketers or datamining companies.[32]

Automated Decisions
A computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making.

Biometric Identifiers
Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.[33]

Controller
Those who direct the purposes and means of how data is processed.[34]

Data Minimization
The principle that any data controller or processor must ensure that the personal data they are processing is:

- adequate – sufficient to properly fulfill the stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – deleted when no longer needed.[35]

Data Protection Agency
An independent agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges.

Explicit Consent

Explicit consent means a freely given, specific, informed and unambiguous indication of wishes by an individual, either by a statement or by a clear affirmative action, signifying clear agreement to personal data relating to them being collected or processed. The statement to obtain explicit consent must specify the nature of the data being collected, the purpose of the collection, the details of any automated decision and its effects, or the details of the data that are going to be processed and the risks of said processing. Explicit consent must be revocable.[36]

Fair Information Practices

The Code of Fair Information Practices were first set out in the 1973 report **Record, Computers, and the Rights of Citizens.** The report was the outcome of a government expert panel, convened by the Department of Health, Education and Welfare (HEW), and chaired by Willis Ware.

The HEW Code of Fair Information Practices are:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[37]

There have been many subsequent articulations of FIPs, the most widely known are the OECD Privacy Guidelines, which were first identified in the 1977 report of the US Privacy Protection Study Commission. The PPSC stated that the eight principles are derived from the US Privacy Act of 1974.

Federal Trade Commission (FTC)

The FTC is a federal agency with a dual mission to protect consumers and promote competition. The FTC develops policy and research tools through hearings, workshops, and conferences. The FTC protects consumers by stopping unfair, deceptive or fraudulent practices in the market place.[38]

General Data Protection Regulation (GDPR)

The European Union's comprehensive privacy law that strengthens data protection, provides new data protection rights to individuals and identifies responsibilities for entities handling personal data. The GDPR applies to all entities that process European consumers' personal data. The framework harmonizes data protection rules across the EU, simplifying legal obligations and providing certainty for businesses. Both the public and private sectors are covered by the GDPR, though the public sector has the benefit of certain exceptions from the law's requirements. Among its many provisions, the rules give data subjects specific new rights from a right to object to a right to information, creates independent supervisory authorities, establishes a new European Data Protection Board, requires a lawful basis for an entity to process any personal data, mandates data breach notification within 72 hours, and enhances penalties for noncompliance up to 4% of global revenue.[39]

Genetic Data

Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.[40]

Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines

The most influential international framework for privacy ever established, as well as one of the most significant contributions of the OECD to the development of international policies for a global economy. The OECD Privacy Guidelines led directly to the adoption of national laws in many countries, including the United States, new business practices, and professional codes of conduct. The Guidelines were originally developed in 1980 and were revised in 2013.[41]

Personal Data

Any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

Personally Identifiable Information (PII)

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name,

address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. [42]

Preemption

Preemption refers to whether a federal law restricts the authority of states, counties, or cities to enact or enforce their own laws. Federal preemption can take two forms—federal floor and federal ceiling preemption. In most consumer and civil rights legislation, federal law serves as a floor of protections. This "federal floor preemption" only supersedes weaker state laws, and it allows states, counties, and local governments to pass stronger laws. An example of federal floor preemption is the Video Privacy Protection Act of 1988, which leaves states free to enact stronger privacy laws. Conversely, "federal ceiling preemption" prevents states and other political entities from passing stronger laws.[43] Federal floor or "baseline" legislation is favored because it allows states to respond to emerging challenges, provides the opportunity for innovative solutions, and reflects the federalist form of U.S. government. Justice Brandeis called the states the "laboratories of democracy," and explained how a "state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[44]

Privacy by Design

"Data protection through technology design." The concept that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created rather than accounting for it after-the-fact.[45]

Privacy Enhancing Techniques ("PETs")

Privacy Enhancing Techniques are techniques that minimize or eliminate the collection of personally identifiable information. PETs enable the development of new services that reduce privacy risk. Data minimization provisions in legislation encourage the promotion of PETs.

Private Right of Action

An individual's right to sue and obtain restitution to enforce rights under a statute.

Processing
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[46]

Processor
An entity that actually process the data on behalf of the data controller.[47]

Profiling
The automated processing of data (personal and not) to derive, infer, predict or evaluate information about an individual or group, in particular to analyze or predict an individual's identity, their attributes, interests or behavior.

Re-identification/De-anonymization
Re-identification is the process by which anonymized personal data is linked to the actual data subject. In some circumstances, computer scientists are able to re-identify anonymized data and link back sensitive information to an individual.[48]

Retention
The holding of data by a data controller or processor.

Statutory Damages
Damages permitted by statute to be paid to a person as compensation for violation of a legal right. Without statutory damages, individual recourse against entities that fail to comply with the statute is limited.[49]

"Take It or Leave It" Terms
Terms that would deny service to an individual who does not approve the collection, use, retention, sharing, or sale of the individual's personal information for commercial purposes on the basis of that lack of approval.[50]

Third Party
Those other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.[51]

ABOUT EPIC

The Electronic Privacy Information Center (EPIC) is a nonpartisan, public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC pursues a wide range of program activities including policy research, public education, conferences, litigation, publications, and advocacy. EPIC routinely files amicus briefs in federal courts, pursues open government cases, defends consumer privacy, organizes conferences for NGOs, and speaks before Congress and judicial organizations about emerging privacy and civil liberties issues. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy.

ENDNOTES

[1] FTC, Consumer Sentinel Network Data Book 2018 (2019), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf.

[2] ForgeRock, *U.S. Consumer Data Breach Report 2019* (June 2019), https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf.

[3] *Id.*

[4] Cable Communications Policy Act of 1984, 42 U.S.C. § 551 (1984).

[5] Electronic Communication Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848–1873 (codified as amended in scattered sections of 18, 28, 47, and 50 U.S.C.).

[6] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1988).

[7] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1998).

[8] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936–2103 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

[9] Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (1991).

[10] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952–2012 (codified as amended in scattered sections of 15 U.S.C.).

[11] Press Release, Eur. Comm'n, EU-U.S. Privacy Shield: Second review shows improvements but a permanent Ombudsperson should be nominated by 28 February 2019 (Dec. 19, 2018), https://europa.eu/rapid/press-release_IP-18-6818_en.pdf; Press Release, Eur. Parl., Suspend EU-US data exchange deal, unless US complies by 1 September, say MEPs (May 7, 2018), http://www.europarl.europa.eu/pdfs/news/expert/2018/7/press_release/20180628IPR06836/20180628IPR06836_en.pdf.

[12] Privacy Shield Framework, 81 Fed. Reg. 51,041, 51,046 (Aug. 2, 2016).

[13] *EU-U.S. Privacy Shield Renewed, Privacy Commitments Ignored*, EPIC (Dec. 19, 2018), https://epic.org/2018/12/eu-us-privacy-shield-renewed-p.html.

[14] EPIC, *Public Opinion on Privacy*, https://epic.org/privacy/survey.

[15] Pew Research Center, *Americans' complicated feelings about social media in an era of privacy concerns* (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[16] Pew Research Center, The state of privacy in post-Snowden America (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[17] Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[18] Press Release, FTC, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network, (Mar. 20, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

[19] Press Release, FTC, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy.

[20] Letter from Senators Edward Markey, Josh Hawley, and Richard Blumenthal to the Honorable Joseph Simons, Chairman, FTC, et al. (Jul. 16, 2019), https://www.markey.senate.gov/imo/media/doc/FTC%20Facebook%20Settlement%20Letter%20.pdf ("We believe that the reported settlement is woefully inadequate. It is clear that a $5 billion fine alone is a far cry from the type of monetary figure that would alter the incentives and behavior of Facebook and its peers. We are concerned that the FTC has failed to put an end to Facebook's privacy invasions.").

[21] California Consumer Protection Act ("CCPA"), Cal. Civ. Code § 1798.100 - 1798.199.

[22] *State Laws Related to Internet Privacy*, Nat'l Conf. of State Leg. (Aug. 13, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

[23] *See* OECD, *The OECD Privacy Framework* (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[24] EPIC, *EU General Data Protection Regulation*, https://epic.org/international/gdpr/.

[25] *See* EPIC, *Council of Europe Privacy Convention*, https://epic.org/privacy/intl/coeconvention/.

[26] EPIC, *Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor")*, https://epic.org/privacy/intl/schrems/.

[27] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, FTC File No. 1823109 at 17 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[28] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

[29] Privacy Act of 1974, 5 U.S.C. § 552a.

[30] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, ch. 13 (1977), https://epic.org/privacy/ppsc1977report/.

[31] EPIC, *Algorithmic Transparency: Ending Secret Profiling*, https://epic.org/algorithmic-transparency/.

[32] EPIC, *Re-identification*, https://epic.org/privacy/reidentification/.

[33] Regulation (EU) 2016/679, *General Data Protection Regulation*, 2016 O.J. (L 119) 34.

[34] *Id.* at 33.

[35] *Guide to the General Data Protection Regulation (GDPR)*, Info. Comm'r's Off. (2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

[36] *Guide to the General Data Protection Regulation (GDPR)*, Info. Comm'r's Off. (2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.

[37] EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.

[38] FTC, *What We Do*, https://www.ftc.gov/about-ftc/what-we-do.

[39] EPIC, *EU General Data Protection Regulation*, https://epic.org/international/gdpr/.

[40] Regulation (EU) 2016/679, *General Data Protection Regulation*, 2016 O.J. (L 119) 34.

[41] *The OECD Privacy Framework* (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[42] 2 C.F.R. § 200.79 (2014).

[43] EPIC, *Privacy Preemption Watch*, https://epic.org/privacy/preemption/.

[44] *New State Ice Co. v. Liebmann*, 285 U.S. 262 (1932).

[45] *What does data protection 'by design' and 'by default' mean?*, Eur. Comm'n, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

[46] Regulation (EU) 2016/679, *General Data Protection Regulation*, 2016 O.J. (L 119) 33.

[47] *Id*.

[48] EPIC, *Re-identification*, https://epic.org/privacy/reidentification/.

[49] *Statutory Damages*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see Damages*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[50] Privacy Bill of Rights Act, S. 1214, 116th Cong. § 8 (2019).

[51] Regulation (EU) 2016/679, *General Data Protection Regulation*, 2016 O.J. (L 119) 34.


epic.org
ELECTRONIC PRIVACY
INFORMATION CENTER