Multicultural Media, Telecom and Internet Council
1250 Connecticut Ave NW, 7th Floor
Washington, D.C. 20036
Phone: 202-261-6543| MMTConline.org

Memorandum on Privacy Regulations in the U.S.

MMTC Spring 2023

Alexandra Cohen, Henry Rivera Fellow

May 23, 2023

Table of Contents

Introduction to Privacy

When we discuss "Privacy Law," we are generally referring to "the laws regulating the collection, storage, and use of personal information."[1] But privacy as a legal concept is amorphous, "encompassing. . .freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[2] Despite the difficulty in articulating exactly what privacy is, its importance is obvious, evidenced by its' explicit protection in many states' and countries constitutions.[3]

The foundation of many traditional privacy laws originated in the 1970's in what is called the Fair Information Practice Principles ("FIPPS").[4] The FIPPS "are a set of internationally recognized best practices for addressing data privacy concerns" which were initially established by the Secretary's Advisory Committee on Automated Personal Data Systems in their 1973 report "Records, Computers and the Rights of Citizens."[5] This report was developed in an effort to understand "many of the problems arising from the application of computer technology to record keeping about people."[6] In the report, the Advisory Committee urged Congress to adopt a "Code of Fair Information Practices" based on five principles:

(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.[7]

Presently, these may be referred to as transparency, use limitation, access and correction, data quality, and security.[8] The principles represent a blend of substantive (data quality, use limitation) and procedural (consent, access) principles.[9] Further, the principles attempt to balance "the need for broad standards to facilitate both individual privacy and the promise of information flows in an increasingly technology-dependent, global society."[10]

The FIPPs have remained a core basis for policy law internationally since their inception. The U.S. codified the FIPPs in a large part in the U.S. Privacy Act of 1974, other countries and regions have since adopted data privacy laws and

[1] Georgetown Law, *Privacy Harms*, Georgetown, https://www.law.georgetown.edu/your-life-career/career-exploration-professional-development/for-jd-students/explore-legal-careers/practice-areas/privacy-law/#:~:text=Privacy%20law%20can't%20easily,and%20use%20of%20personal%20information.
[2] Daniel Solove, *Understanding Privacy* 1 (2008).
[3] *Id.* at 2-3.
[4] *See* John Kropf, *A Short History of the Fair Information Practice Principles as a Foundation for Personal Data Sharing Across Borders*, Privacy Across Borders 1 (July 8, 2022) https://privacyacrossborders.org/wp-content/uploads/2022/07/A-Short-History-of-the-Fair-Information-Practice-Principles-as-a-Foundation-for-Personal-Data-Sharing-Across-Borders.pdf
[5] Secretary's Advisory Committee on Automated Personal Data Systems, NO.(OS)73-94, *Records, Computers, and the Rights of Citizens* (1973).
[6] *Id.* at iii.
[7] *Id.* at xx-xxi.
[8] Fred H. Cate, *The Failure of fair Information Practice Principles*, Consumer Protection in the Age of the Information Economy 346 (2006).
[9] *Id.* at 343.
[10] *Id.*

guidance that reflect the FIPPs.[11] As we discuss federal, state, and international privacy laws, it will be easy to see the continuing impact of the FIPPs.

Overview of Relevant Privacy Regulations

Privacy regulation in the U.S. may best be described as a patchwork of laws. There is no one national privacy law which regulates the collection and use of personal information generally. Instead, there are several federal sectorial privacy laws. Sectorial privacy laws are laws that are specific to a certain "sector" and cover relevant personal information as defined under that regulation. For instance, certain kinds of health information are protected under HIPAA while banks are regulated under another law, GLBA. Basically, on a federal level, one individual's personal information is generally regulated by a series of laws.

What is left unregulated by the federal government is left to the state to decide whether and how to regulate. There are several state specific privacy laws; some are more general privacy laws, such as the California Consumer Protection Act, and others apply to specific kinds of personal information, such as the Illinois Biometric Information Privacy Act. The following is a brief introduction to sectorial, state, and relevant international privacy regulations.

[11] Kropf *supra* note 4 at 1.

Federal Privacy Regulations

Children's Online Privacy and Protection Act (COPPA)

In 1998, Congress enacted The Children's Online Privacy and Protection Act (COPPA) which "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet."[12] Specifically, COPPA applies to "operators of websites and online services that collect personal information from kids under 13."[13] Before discussing the obligations imposed by COPPA, it is helpful to first determine what entities are covered by COPPA.

COPPA AT A GLANCE

Regulates: "Operators of commercial websites and online services directed to children under 13"
Mission: Consumer Protection
Law: 15 U.S.C. §§ 6501-6506. Pub. L. 105-277

First, what does "operators of websites and online service's" mean? The FTC provides helpful criteria in determining who must comply with COPPA:

1. "Your website or online service[14] is directed to children under 13 and you collect personal information from them; **OR**
2. Your website or online service is directed to children under 13 and you let others collect personal information from them; **OR**
3. Your website or online service is directed to a general audience, but you have actual knowledge that you collect personal information from children under 13; **OR**
4. Your company runs an ad network or plug-in, for example, and you have actual knowledge that you collect personal information from users of a website or service directed to children under 13."[15]

However, COPPA does not apply to nonprofit entities that would be exempt from coverage under Section 5 of the FTC Act.[16] Further, foreign-based websites and online services *must* comply with COPPA if those sites (1) are directed to children in the U.S., or (2) knowingly collect personal information from children in the U.S.[17] Still, it is best practice for all websites that collect personal information to post privacy policies on their site and to provide COPPA's protections.

Next, what does it mean for an online service to be "directed to children under 13"? Some websites target children as their primary audience and would clearly be covered under this criteria, however, even websites that do not primarily target children may still be directed to children under 13.[18] The FTC considers various factors to make this determination such as: the subject matter of the site or service, visual and audio content, the use of animated characters or other child-oriented activities and incentives, the age of models, the presence of child celebrities or celebrities who appeal to

[12] *See* 15 U.S.C. §§ 6501-6505; 16 C.F.R. § 312.1.
[13] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, FTC Business Guidance (Mar. 20, 2015) https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions
[14] *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step1 (Defining "website or online service").
[15] *Id.*
[16] Sean Meyers, *Guide to COPPA*, Privacy Policies (Jul. 01, 2022) https://www.privacypolicies.com/blog/coppa/; *see FTC v. California Dental Association*, 526 U.S. 756 (1999)
[17] 16 C.F.R. § 312.2; *Supra* note 6.
[18] 16 C.F.R. §312.2.

kids, and other reliable evidence about the age of the actual or intended target audience.[19] Websites that don't target children as its primary audience may choose to apply COPPA protections only to users under age 13.[20]

Finally, what kinds of information is covered? COPPA deals with the collection of "personal information" which it defines as including:

- First and last name
- Social security number
- Online contact information
- A telephone number
- A home or other physical address including street name and name of a city or town
- A screen or username that functions as online contact information
- A photograph, video, or audiofile, where such file contains a child's image or voice
- Geolocation information sufficient to identify street name and name of a city or town
- A persistent identifier that can be used to recognize a user over time and across different websites or online services
- Information concerning the child or he parents of that child that the operator collects online from the child and combines with an identifier described above.[21]

With these definitions in mind, we will move on to the requirements that COPPA imposes on covered entities. The main requirements for websites include:

1. A detailed privacy policy that describes the information collected from its users
2. Obtaining verifiable parental consent prior to collection of personal information from a child under 13
3. Disclose to parents any information collected on their children by the website
4. Ensure a Right to revoke consent and have information deleted
5. Limited collection of personal information when a child participates in online games and contests
6. A general requirement to protect the confidentiality, security, and integrity of any personal information that is collected online from children[22]

COPPA requires covered entities to provide several forms of notice, one is a direct notice to parents, covered under §312.4(c), the other notice is a prominent and clearly labeled link to an online notice of information practices.[23] The following information must be included:

1. A list of all operators collecting personal information. The name, address, telephone number, and email address of all operators collecting or maintaining personal information through the site or service (or, after listing all such operators, provide the contact information for one that will handle all inquiries from parents);
2. A description of what information the operator collects from children, including whether the operator enables children to make their personal information publicly available, how the operator uses such information, and the operator's disclosure practices for such information; and
3. That the parent can review or have deleted the child's personal information and refuse to permit its further collection or use and further state procedures for doing so.[24]

Further, the link to the policy should be on the homepage and any page that collects personal information.[25] The links should be clear and prominent, the FTC suggests using a larger font or a different color type on a contrasting background.[26] The policy itself should be clear and easy to read without any unrelated or confusing information.[27]

---

[19] *Id.*
[20] *Id.*
[21] *Id.* at "Personal Information".
[22] *Children's Privacy*, Electronic Privacy Information Center, https://epic.org/issues/data-protection/childrens-privacy/
[23] § 312.4(c),(d); § 313.4(a)
[24] FAQ; 16 C.F.R § 312.4(d).
[25] §312.4(d).
[26] Federal Trade Commission, *supra note* 16.
[27] *Id.*

Beyond the notice, websites must obtain "parents' verifiable consent before collecting personal information from their kids." The Rule provides a roadmap of what information must be included in the direct notice in four specific instances:

1. Where an operator collects the name or online contact information of a parent or child in order to obtain a parent's verifiable consent prior to the collection, use, or disclosure of a child's personal information.
2. Where an operator voluntarily seeks to provide notice to a parent of a child's online activities that do not involve the collection, use, or disclosure of personal information.
3. Where an operator intends to communicate with the child multiple times via the child's online contact information and collects no other information.
4. Where the operator's purpose for collecting a child's and a parent's name and online contact information is to protect a child's safety and the information is not used or disclosed for any other purpose.

The specifics of what information must be provided in each situation can be found in §312.4(c)(1)-(4) and in the FTC's *Complying With COPPA*. As far is *how* to obtain consent, COPPA leaves it up to the operator, but the FTC advises choosing a method reasonably designed in light of available technology to ensure that the person giving the consent is actually the parent.[28] However, the list of acceptable methods includes:

- A consent form signed and sent back via fax, mail, or electronic scan;
- Use of a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
- A toll-free number staffed by trained personnel;
- A copy of a form of government issued ID checked against a database, *so long as* the identification is deleted once the verification process is complete;
- A series of knowledge-based challenge questions geared towards the parent; or
- Verifying a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.

Finally, COPPA requires that operators establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected by children.[29] A general best practice is to minimize what data is collected in the first place.[30] COPPA additionally states that operators of a website or online service must only retain a child's personal information "for as long as is reasonably necessary to fulfill the purpose for which the information was collected."[31]

Enforcement

Generally, violations of COPPA are considered to be unfair or deceptive trade practices under §5 of the FTC Act, which is the primary enforcement mechanism of the Rule.[32] Additionally, COPPA gives states and certain federal agencies, such as the Office of the Comptroller of the Currency and the Department of Transportation, authority to enforce compliance with respect to entities over which they have jurisdiction.[33] Finally, at the state level, COPPA authorizes state attorneys general to bring actions in federal district court to enforce compliance with the act and to obtain damages or some other form of relief.[34]

---

[28] *Id.*
[29] §312.8.
[30] *See generally* Bernard Marr, *Why Data Minimization is An Important Concept in the Age of Big Data*, Forbes (Mar. 16, 2016) https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=6ff3e6681da4.
[31] §312.10.
[32] § 312.9.
[33] Federal Trade Commission, *supra note* 16.
[34] *Id.*

A court may hold operators who are found to have violate the Rule liable for civil penalties of up to $46, 517 per violation.[35] The determination of the appropriate civil penalty will vary by case, in some instances, the FTC has sought no civil penalty.[36] The amount sought will depend on a number of factors, such as the egregiousness of the violation, whether the operator as previously violated the Rule, the number of children involved, the amount and type of the personal information collected, how the information was used, whether it was shared with third parties, and the size of the company.

For More Information:

- Text of the Act
- Federal Trade Commission, Complying with COPPA: Frequently Asked Questions
- International Association of Privacy Professionals, COPPA

[35] *Id.*
[36] *Id.*

Fair Credit Reporfiting Act (FCRA)

The Fair Credit Reporting Act was enacted in 1970 to "insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[37] In 2003, the FCRA was amended by the Fair and Accurate Credit Transactions Act (FACTA) in an effort to enhance consumer protections, particularly in relation to identity theft – the Gramm-Leach-Bliley Act (GLBA) made additional changes as well.[38] This section is a discussion of the FCRA as amended by FACTA and the GLBA. FCRA is an incredibly lengthy and complex law – this discussion is not meant to be a comprehensive presentation of all rights and obligations under FCRA.

FCRA AT A GLANCE

Regulates: Consumer Reporting Agencies, Users of Consumer Reports, Creditors of Consumer Information
Mission: Consumer Protection
Law: 15 U.S.C. § 1681 *et seq.*
Pub. L. 91-508

Ultimately, FCRA governs how credit bureaus can collect and share information about individual consumers,[39] such as regulating *how* a consumer's credit information is obtained, how long that information is kept, and how that information is shared with others. Credit bureaus, or consumer reporting agencies (CRA), are defined under the act as:

> any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.[40]

The FCRA generally regulates (1) consumer reporting agencies;[41] (2) users of consumer reports; (3) and furnishers of consumer information. Additionally, the FCRA limits what kinds of data can be collected and used in credit reports. First, a consumer report is any written or oral communication that meets all the following conditions:

- It was prepared by a Credit Reporting Agency;
- Pertains to a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living
- Is used, at least in part, to establish a consumer's eligibility for:
    - Credit or insurance for personal, family, or household purposes;
    - Employment purposes;[42] or
    - Any other purpose authorized under § 1681b.[43]

There is some information that is excluded from the definition of a credit report. Specifically, "transaction and experience" information, or records of goods and services, are excluded.

Individual Rights

[37] 15 U.S.C. § 1681(a)(4).
[38] *Fair and Accurate Credit Transactions Act of 2003*, Federal Trade Commission, https://www.ftc.gov/legal-library/browse/statutes/fair-accurate-credit-transactions-act-2003
[39] § 1681a(c) (The term "consumer" means an individual).
[40] § 1681a(f).
[41] There are three national CRA's in the United States: Experian, Trans Union, and Equifax.
[42] § 1681(a)(g) (The term "employment purposes" when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee).
[43] § 1681a(d)(1)(A)-(C).

The right to know if information in your file has been used against you. Anyone who uses a credit report or other type of consumer report to deny an individual's application for credit, insurance, or employment, must tell that individual as well as provide the name, address, and phone number of the agency that provided the information.[44]

The right to know what is in your file. Individuals may request and obtain all information about them in the files of a CRA.[45] Upon request, the CRA must clearly and accurately disclose to the consumer:

- All information in the consumer's file at the time of the request;
- Identification of each person that procedure a consumer report during the 2-year period preceding the date of the request if for employment purposes, or during the 1-year preceding the date of the request for any other purpose;[46]
    - Identification must include: (1) the name of the person or, if applicable, the trade name under which such person conducts business; and (2) upon request of the consumer, the address and telephone number of the person.
- The dates, original payees, and amounts of any checks upon which is based any adverse characterization of the consumer;
- A record of all inquiries received by the agency during the 1-year period preceding the request that identified the consumer in connection with a credit or insurance transaction that was not initiated by the consumer;
- If the consumer requests the credit file and not the credit score, a statement that the consumer may request and obtain a credit score.

Consumers may request up to one free report from CRA's during any 12-month period.[47] Further, CRA's must fulfill this request within 15 days.[48]

The right to ask for a credit score. Individuals may request a credit score from consumer reporting agencies, but they will likely have to pay for it.[49]

The right to dispute incomplete or inaccurate information. If an individual identifies information in their file that is incomplete or inaccurate, and subsequently reports it to the CRA, the agency must investigate the claim and remove inaccurate information.[50]

Obligations on Consumer Reporting Agencies

In addition to actualizing the individual rights listed above, CRA's are subject to additional requirements under the CRA – this section will provide only a brief overview of these obligations. First, CRA's may provide consumer reports only under certain circumstances:

---

[44] *See* § 1681(a)(k),(y); § 1681b(b)(3)(A).
[45] § 1681g(a); *See also* Consumer Financial Protection Bureau, *A Summary of Your Rights Under the Fair Credit Reporting Act* (n/a) https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf
[46] § 1681g(a)(3).
[47] § 1681j(a)(1)(A); *see also* § 1681j(a)(1)(B) ("Subparagraph (A) shall apply with respect to a consumer reporting agency described in section 603(p) only if the request from the consumer is made using the centralized source established for such purpose in accordance with section 211(c) of the Fair and Accurate Credit.").
Transactions Act of 2003.
[48] § 1681j(a)(2).
[49] *Id.*
[50] *Id.*

1. In response to the order of a court, a subpoena issued in connection with proceedings before a Federal grand jury, or a subpoena issued in accordance with § 5318 of Title 31 or § 3486 of Title 18.
2. In accordance with the written instructions of the consumer to whom it related.
3. To a person which it has reason to believe
    a. Intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished;
    b. Intends to use the information for employment purposes;
    c. Intends to use the information in connection with the underwriting of insurance
    d. intends to use the information). in connection with a determination of the consumer's eligibility for a license;
    e. Intends to use the information, as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; or
    f. Otherwise has a legitimate business need for the information
        i. in connection with a business transaction that is initiated by the consumer; or
        ii. to review an account to determine whether the consumer continues to meet the terms of the account.
    g. Executive departments and agencies in connection with the issuance of government-sponsored individually-billed travel charge cards.
4. In response to a request by the head of a State or local child enforcement agency, if the person making the request makes certain assurances to the CRA.
5. To an agency administrating a state plan for use to set an initial or modified child support award.
6. To the Federal Deposit Insurance Corporation or the National Credit Union Administration as part of its preparation for its appointment or as part of its exercise of powers, as conservator, receiver, or liquidating agent for an insured depository institution or insured credit union under the Federal Deposit Insurance Act or the Federal Credit Union Act.[51]

Additionally, CRA's are regulated in when they may furnish a consumer report for employment purposes. In order to do so:

- The person who is obtaining the report from the CRA must certify that:
    - The person has provided a clear and conspicuous disclosure, in writing, at any time before the report is procured or caused to be procured, that a consumer report may be obtained for employment purposes and the consumer has provided authorization in writing; and
    - The information will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.
- The CRA must provide with the report, or has previously provided, a summary of the consumer's rights.[52]

Obligations on Furnishers of Information

The FCRA uses the same definition of a creditor as found in the Fair Credit Opportunity Act. A creditor is:

> Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit, or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.[53]

[51] § 1681b(a)(1)-(6).
[52] § 1681b(b)(1).
[53] § 1681a(e).

In other words, a creditor is a company that furnishes information to consumer reporting agencies, and typically has some sort of credit agreement with a consumer (e.g. credit card companies or auto finance companies).[54] The obligations that the FCRA imposes upon furnishers of information largely relate to their:

1. Duty to Provide Accurate Information;[55] and
2. Duties After Receiving Notice of a Dispute.

Duty to Provide Accurate Information

As part of their duty to provide accurate information to a consumer reporting agency, furnishers are prohibited from both reporting information with *actual knowledge*[56] of errors, and reporting information after *notice and confirmation* of errors.[57]

Section 1681s-2(a) additionally delineates other duties on furnishers of information that correspond with their duty to provide accurate information. Those include:

Duty to correct and update information. Once a furnisher of information determines that information it has furnished to a CRA is not complete or accurate, it must promptly notify the CRA of that determination and provide any corrections or additional information that is necessary to make the information complete and accurate.[58]

Duty to provide notice of dispute. A furnisher of information must provide notice that information is disputed by the respective consumer or else cannot furnish said information.[59]

Duty to provide notice of closed accounts. A furnisher of information must notify the CRA of any voluntary closure of a credit account by the consumer, in information regularly furnished for the period in which the account is closed.[60]

Duty to provide notice of delinquency of accounts. A furnisher of information to a CRA regarding a delinquent account being placed for collection, charged to profit or loss, or subjected to any similar action must notify the CRA of the date of delinquency on the account, within 90 days.[61]

Duties upon notice of identity theft-related information. A furnisher of information must put into place reasonable procedures to respond to notifications that it receives from a CRA relating to information resulting from identity theft.[62] The furnisher is prohibited from furnishing information related to an identity theft report submitted by a consumer, unless it is confirmed that the information is accurate and complete.[63]

Duty to provide notice upon furnishing negative information. Where a furnisher of information provides negative information to a CRA regarding credit extended to a consumer, the furnisher must provide a notice, in writing, to the

[54] Other examples of information furnishers are collection agencies, state or municipal courts reporting a judgment, or past and present employers.
[55] *See generally* § 1681s-2(a).
[56] *Id.* at (A) ("A person shall not furnish any information relating to a consumer to any consumer reporting agency if the person knows or has reasonable cause to believe that the information is inaccurate."); See also 15 U.S.C. § 1681s-2(D) ("[T]he term "reasonable cause to believe that information is inaccurate" means having specific knowledge, other than solely allegations by the consumer, that would cause a reasonable person to have substantial doubts about the accuracy of the information.").
[57]
[58] § 1681s-2(a)(2)(B).
[59] § 1681s-2(a)(3).
[60] § 1681s-2(a)(4).
[61] § 1681s-2(a)(5).
[62] § 1681s-2(a)(6)(A).
[63] *Id.* at (B).

consumer, within 30 days.[64] Negative information is defined as "information concerning a customer's delinquencies, late payments, insolvency, or any form of default."[65]

Duty to provide notice of status as medical information furnisher. A furnisher of information whose primary business is providing medical services, who furnishes information to a CRA on a consumer is considered a medical information furnisher and must notify the CRA of that designation.[66]

Duties Upon Notice of Dispute

After receiving notice of a dispute with regard to the completeness or accuracy of information on a consumer, the furnisher of information must:

1) Conduct an investigation with respect to the disputed information;
2) Review all relevant information provided by the CRA;
3) Report the results of the investigation to the CRA;
4) If the information is found to be incomplete or inaccurate, report those results to all other CRAs to which the furnisher sent the information and that compile and maintain files on consumers on a nationwide basis; and
5) If information disputed by a consumer is found to be inaccurate, incomplete, or cannot be verified after any reinvestigation, for purposes of reporting to a CRA only, as appropriate:
    a. Modify that item of information;
    b. Delete that item of information; OR
    c. Permanently block the reporting of that item of information.[67]

The FTC provides a more complete guide on the obligations of Information Furnishers which can be found here.

Obligations on Users of Consumer Reports

Users taking adverse actions against the consumer based on the information of information contained in the consumer reports have specific duties under 15 U.S.C. § 1681m. These users must:

- Provide oral, written, or electronic notice of the adverse action to the consumer;
- Provide to the consumer written or electronic disclosure of a numerical credit score and the information set forth in subparagraphs (B) through € of section 609(f)(1).
- Provide to the consumer orally, in writing, or electronically:
    - The name, address, and telephone number of the CRA that furnished the report to the person; and
    - A statement that the CRA did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken; and
- Provide to the consumer an oral, written, or electronic notice of the consumer's right
    - To obtain a free copy of a consumer report; and
    - To dispute with a CRA the accuracy or completeness of any information in a consumer report furnished by the agency.[68]

Additionally, a consumer has the right to request reasoning for adverse action being taken against them, where that action is based on information obtained from third parties other than CRA's.[69] The consumer must submit a written

[64] § 1681s-2(a)(7)(A),(B).
[65] § 1681s-2(a)(7)(G).
[66] § 1681s-2(9).
[67] § 1681s-2(b)(1)(A) – (E).
[68] § 1681m(a)(1)-(4).
[69] § 1681m(b)(1).

request within 60 days after learning of the adverse action, and the user of such information must clearly and accurately disclose to the consumer their right to make that request when the adverse action is disclosed to the consumer.[70]

Any user of a consumer report who uses that report in connection with a credit or insurance transaction that is not initiated by the consumer, must provide with each written solicitation made to the consumer regarding the transaction a clear and conspicuous statement that:

- Information contained in the consumer's consumer report was used in connection with the transaction;
- The consumer received the offer of credit or insurance because the consumer satisfied the criteria for credit worthiness or insurability under which the consumer was selected for the offer;
- If applicable, the credit or insurance may not be extended if, after the consumer responds to the offer, the consumer does not meet the criteria used to select the consumer for the offer;
- The consumer has a right to prohibit information contained in the consumer's file with any CRA from being used in connection with any credit or insurance transaction that is not initiated by the consumer, and the consumer may exercise this right through a notification system established under § 1681b.[71]

Enforcement

The FTC and the Consumer Financial Protection Bureau (CFPB) are the two federal agencies charged with overseeing and enforcing the FCRA.[72] FCRA splits noncompliance penalties between willful noncompliance and negligent noncompliance.[73]

Any person who willfully fails to comply with any requirement under the FCRA with respect to any consumer is liable to that consumer in an amount equal to the sum of (1) punitive damages as determined by the court, attorney's fees,[74] and:

- Any actual damages sustained by the consumer not less than $200 and not more than $1,000; or
- In the case of liability of a natural person for obtaining a consumer report under *false pretenses* or knowingly without a permissible purpose, actual damages sustained by the consumer or $1,000, whichever is greater;[75]

Where a person is negligent in failing to comply with any requirement under the FCRA with respect to any consumer, that person is liable in an amount equal to the sum of:

- Any actual damages sustained by the consumer as a result of the failure; and
- The costs of the action with reasonable attorney's fees as determined by the court.[76]

Any action to enforce the FCRA must be brought no later than either (1) 2 years after the date of discovery by the plaintiff of such liability or (2) 5 years after the date on which the violation occurs, *whichever is earlier*.[77]

[70] *Id.*
[71] § 1681m(d)(1)(A)-(E).
[72] § 1681s(a),(b).
[73] *See generally* §§ 1681n, 1681o.
[74] *See* § 1681n(c) ("Upon a finding by the court that an unsuccessful pleading, motion, or other paper filed in connection with an action under this section was filed in bad faith or for purposes of harassment, the court shall award to the prevailing party attorney's fees reasonable in relation to the work expended in responding to the pleading, motion, or other paper.").
[75] § 1681n(a)(1)(A),(B).
[76] § 1681o(a)(1),(2).
[77] § 1681p.

Further, the FTC is authorized to enforce the FCRA with respect to consumer reporting agencies, as an unfair or deceptive act or practice under section 5(a) of the FTC Act.[78] Section 1681s additionally outlines liability under the FCRA with respect to enforcement actions by federal agencies.[79]

For More Information:

- Text of the Act
- Consumer Financial Protection Bureau, A Summary of Your Rights Under the Fair Credit Reporting Act
- Federal Trade Commission, Consumer Guide on Credit Reports
- CRS Report, Fair Credit Reporting Act: Rights and Responsibilities

[78] § 1681s(a)(1).
[79] *See generally* § 1681s.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) of 1974 is a federal law that parents and eligible students specific rights concerning personally identifiable information from their education records.[80] FERPA was signed into law on August 21, 1974 – it was enacted as § 444 of the General Education Provisions Act (GEPA) called "Protection of the Rights and Privacy of Parents and Students" and codified 20 U.S.C. § 1232g.[81] Subsequent regulations were promulgated by the Secretary of Education and may be found in 34 C.F.R. Part 99.

FERPA AT A GLANCE

Regulates: Educational Institutions
Mission: Student Privacy
Law: 20 U.S.C. § 1232g; 34 C.F.R. Part 99

Covered educational agencies or institutions may be found under 34 C.F.R. §99.1 but generally, FERPA applies "to any public or private elementary, secondary, or post-secondary school and any state or local education agency that receives federal funds under a program administered by the Secretary of Education."[82]

FERPA can be split into two separate parts. First, FERPA gives parents and eligible students certain rights, including the right to review their own education records and request corrections. Second, it prohibits educational institutions from disclosing "personally identifiable information in education records" without the written consent of eligible students or parents. Each part will be discussed in greater detail. First, it is helpful to define a few key terms in the Act.

There are two criteria which must be met for a document to be considered part of an education record: that the record (1) must "directly relate" to a student; and (2) must be "maintained by an educational agency or institution by a person acting for such agency or institution."[83] The FERPA explicitly includes certain kinds of records from its definition of an "education record" such as: alumni records, records used as personal memory aids, and records of the law enforcement unit of an educational agency or institution.[84]

To understand this designation, there is still clarification needed. Let's start with discussing the significance of "directly relate." FERPA regulations do not define what it means for a record to be "directly related" to a student. However, the Department of Education provides examples of education records, such as grades, transcripts class lists, health records, and student discipline files.[85] Next, what does it mean for a record to be "maintained by an education agency"? The Supreme Court has described education records as "institutional records kept by a single central custodian,

[80] 34 C.F.R. Part 99; https://studentprivacy.ed.gov/faq/what-ferpa
[81] *See generally General Education Provisions Act (GEPA): Overview and Issues*, Every CRS Report (Mar. 18, 2010) https://www.everycrsreport.com/reports/R41119.html#_Toc256753055.
[82] N/A. *Family Educational Rights and Privacy Act (FERPA)*, Electronic Privacy Information Center (EPIC), https://epic.org/family-educational-rights-and-privacy-act-ferpa/; 34 C.F.R. § 99.1(a); *see also* 33 C.F.R. § 99.1(c) (Defining what the Secretary considers to be funds made available to an educational agency or institution).
[83] 20 U.S.C. § 1232g(a)(4)(A); 34 C.F.R. § 99.3.
[84] 20 U.S.C. § 1232g(a)(4)(B).
[85] U.S. Dept. of Ed., *Frequently Asked Questions*, StudentPrivacy.ed.gov, https://studentprivacy.ed.gov/frequently-asked-questions; *see also Bracco v. Machen*, Np. 01-2009-CA-4444 (Fla. Cir. Jan. 10, 2011) (myfloridalegal.com) (Holding that recordings of student senate meetings are not educational records under FERPA as the proceedings did not relate directly to an identified student, covered generally topics of importance to students, and because the meeting itself was open).

such as a registrar. . ."[86] In essence, to be covered by FERPA, the record must be systematically maintained by the school.[87]

FERPA defines the term personally identifiable information (PII) to include direct identifiers (a student's or other family member's name) and indirect identifiers (a student's date of birth, place of birth, etc.).[88] Indirect identifiers, metadata about students' interaction with an app or service, and even aggregate information can be considered PII under FERPA if a reasonable person in the school community could identify individual students based on the indirect identifiers together with other reasonable available information, including public information.

Disclosures

As a basic rule, the disclosure of education records requires the written consent of the parent or eligible student.[89] Written consent must:

1. Be signed and dated
2. Specify what records are to be disclosed
3. State the purpose of the disclosure
4. Identify the party or class of parties to whom the disclosure may be made.[90]

There are permissible disclosures allowed by FERPA. These disclosures, listed under §99.31, are *voluntary* as opposed to *mandated*.[91] For instance, a school *may* disclose protected information in a health or safety emergency so long as there is an articulable and significant threat to the health or safety of the student or others.[92] Further, schools may disclose "directory" information such as a students name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must inform parents and eligible students about directory information in addition to providing them a reasonable amount of time to request that the school not disclose their information.

Ultimately, instances where schools may disclose education records without prior consent *includes* but is not limited to:

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student, *in certain circumstances*;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.[93]

---

[86] *Owasso Indep. Sch. Dist. No. I-011 v. Falvo*, 534 U.S. 426, 435 (2002).

[87] The following are examples of records that are *not* centrally maintained and subject to FERPA: quiz papers and assignments that are graded in-class by other students, E-mails about students stored on individual teachers; hard drives or sent between student and advisors, blog posts, single copies of teacher's notes, photos and videos taken on school property. https://splc.org/ferpa-what-it-means-and-how-it-works/

[88] 34 C.F.R. §99.3; U.S. Dept. of Ed., *Personally Identifiable Information for Education Records*, studentprivacy.ed.gov, https://studentprivacy.ed.gov/content/personally-identifiable-information-education-records#:~:text=Personally%20identifiable%20information%20for%20education%20records%20is%20a%20FERPA%20term,birth%2C%20or%20other%20information%20which.

[89] § 99.30(a).

[90] § 99.30(b)(1)-(3).

[91] § 99.31(a).

[92] § 99.32(a)(5).

[93] § 99.32(a).

There are additionally certain record keeping requirements concerning requests and disclosures under §99.32. Ultimately, FERPA's disclosure rules are extensive and dependent on who the disclosure is being made to and for what purpose. FERPA categorizes its disclosure rules as follows:

§ 99.30 – Under what conditions is prior consent required to disclose information?

§ 99.31 – Under what conditions is prior consent not required to disclose information?

§ 99.33 – What limitations apply to the redisclosure of information?

§ 99.34 – What Conditions Apply to Disclosure of Information to Other Educational Agencies or Institutions?

§ 99.35 – What Conditions Apply to Disclosure of Information for Federal or State Program Purposes?

§ 99.36 – What Conditions Apply To Disclosure of Information in Health and Safety Emergencies?

§ 99.37 – What Conditions Apply to Disclosing Directory Information?[94]

§ 99.38 – What Conditions Apply to Disclosure of Information as Permitted by State Statute Adopted After November 19, 1974, Concerning the Juvenile Justice System?

Individual Rights

On request, a school must allow a parent or eligible student to:

1. Inspect and review that student's education record;
2. Schedule a hearing to challenge the content of the record to ensure that it is not inaccurate, misleading, or otherwise in violation of the privacy rights of the student;
3. Receive an annual notice of FERPA rights;
4. Consent to disclosure;
5. Insert into such record a written explanation by the parents recording the content of the record.[95]

There is no right to inspect and review medical treatment records or sole possession records under FERPA.

Enforcement

FERPA There is no private right of action, but parents or eligible students who believe an institution has violated FERPA can file a complaint with the Department of Education's Office of Chief Privacy Officer.[96] If the Office determines that the institution is not in compliance with HIPAA, the Act states that the Office may "take any legally available enforcement action in accordance with the Act, including, but not limited to" the following: (1) withhold further payments under any applicable program; (2) issue a complaint to compel compliance through a cease and desist order; or (3) terminate eligibility to receive funding under any applicable program.[97]

When third parties receiving education records from a school violate FERPA, the FPCO can ban further access to education records by those third parties for a minimum of five years.[98]

[94] *See* § 99.3 "Directory information" (Director Information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed).
[95] § 99.7(a)(2).
[96] § 99.63.
[97] § 99.67(a).
[98] § 99.67(c); *see also* § 99.67(b),(d).

For More Information:

- Text of the Act
- How to File a Complaint
- Teach Privacy, An Overview of Education Privacy
- Teach Privacy, What is an "Education Record" Under FERPA? A Discussion and Flowchart

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted to control the ways financial institutions deal with the private information of individuals.[99] The GLBA repealed large portions of the Glass-Steagall Banking Act of 1933 and the Bank Holding Company Act of 1956.[100] Overall, the Act

requires that all "covered institutions" develop privacy practices and policies that detail how they collect, sell, share, and otherwise reuse customer data.[101]

GLBA AT A GLANCE

Regulates: Financial Institutions
Mission: Consumer Protection
Law: 16 C.F.R. §§ 313, 314; Amended 12 U.S.C., 15 U.S.C.
Pub. L. 106-102

The Act is split into three sections:

1) The Financial Privacy Rule
2) The Safeguards Rule
3) Pretexting Provisions

First, what is a covered institution? In short, GLBA regulates any institution that is "significantly engaged" in financial activities.[102]

Examples of Financial Institutions, § 314.2(h)

- Mortgage Lenders
- Account Servicers
- Credit Counselors & Other Financial Advisors
- Payday Lenders
- Check Cashers
- Tax Preparation Firms
- Financial Companies
- Wire Transferors
- Non-Federally Insured Credit Unions

GLBA applies not only to banks, brokerage firms, and insurers, but also to companies that process loans and those that generally assume credit risk. Two factors to consider in determining whether a business is significantly engaged in financial activities are (1) whether there is a formal arrangement, and (2) how often the business engages in a financial activity.[103] Section 314.2(h) of the Rule lists thirteen examples of the kinds of entities that *are* financial institutions.

Notably, businesses may otherwise be covered by GLBA if they receive nonpublic personal information from a financial institution which they are not affiliated with.[104] GLBA defines nonpublic personal information (NPI) as

1) personally identifiable information; and
2) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable information that is not publicly available.

The Financial Privacy Rule

[99] Garry Kranz, *Gramm-Leach-Bliley Act (GLBA)*, TechTarget, https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act.
[100] *Id.*
[101] *Id.*
[102] 16 C.F.R. § 314.2(h)(1).
[103] Federal Trade Commission, *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, Business Guidance, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act
[104] 16 C.F.R. § 313.1(b).

The financial privacy rule, privacy rule, places certain obligations on how organizations may collect and disclose "nonpublic personal information" to third parties. Obligations of financial institutions under the GLBA depends on whether clients are "customers" or "consumers."

	Definition	Examples
Consumer	someone who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that person's legal representative.[105] *Excludes commercial clients*	1) cashing a check with a check-cashing company 2) making a wire transfer 3) applying for a loan.
Customer	A subclass of consumers who have a **continuing relationship** with the financial institution, it is the *length* of the relationship that is important.[106]	1) opening a credit card account with a financial institution 2) getting a loan from a mortgage lender or payday lender 3) using a mortgage broker to secure financing

The Privacy Notice

GLBA places requirements on financial institutions to provide initial, annual, and revised privacy notices. When the privacy notice must be provided, and what must be contained in it, varies upon whether the recipient is a customer or consumer as defined above. Requirements for Privacy and Opt Out Notices may be found in 16 C.F.R. 313 Subpart A.

Generally, all privacy notices must be "clear and conspicuous," which the FTC defines as:

> It must be reasonably understandable, and designed to call attention to the nature and significance of the information. The notice should use plain language, be easy to read, and be distinctive in appearance. A notice on a website should be placed on a page that consumers use often, or it should be hyperlinked directly from a page where transactions are conducted.[107]

Principally, if a financial institution plans to disclose NPI about its' consumers (customer or not) to a nonaffiliated third party, and an exception does not apply, the institution must provide to its consumer:

- an initial notice of its privacy policies;
- an opt-out notice, which includes a reasonably means to opt out; and
- A reasonably opportunity, before the disclosure of NPI, to opt out.

Further, the financial institution must provide a revised notice before the financial institution begins to share a new category of NPI or begins to share information with a new category of nonaffiliated third party in a matter not described in a prior notice.[108]

While specific requirements of a privacy notice vary depending on who it is provided to (customer v. consumer), and what kind it is (initial, annual, revised), each notice must include:

1) Categories of nonpublic personal information collected, categorized as:

[105] § 313.3(e)(1).
[106] § 313.3(h)
[107] Federal Trade Commission, *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*.
[108] § 313.8(a).

a) Information about the consumer;
b) Information about the consumer's transactions with a financial institution or its affiliates; or
c) Information about the consumer's transactions with non-affiliated third parties;
d) Information from a CRA.[109]

2) Categories of nonpublic personal information disclosed;

3) Categories of affiliates and nonaffiliated third parties to who the information is disclosed;

4) Categories of affiliates and nonaffiliated third parties to whom the NPI is disclosed;

5) If the financial institution is disclosing NPI to nonaffiliated third parties under the exceptions in § 313.14 and § 313.15, the privacy notice must include a separate statement of the categories of information disclosed AND the categories of third parties;

6) An explanation of consumers' and customers' right to opt out if the institution is disclosing NPI to nonaffiliated third parties, including the method(s) by which the consumer may opt-out;

7) Any disclosures the financial institution makes under § 603(d)(2)(A)(iii) of the Fair Credit Reporting Act;.

8) The financial institution's policies and practices with respect to protecting the confidentiality and security of NPI; and

9) Any disclosure made under paragraph (b) of this section.[110]

Of the above requirements, the financial institution only needs to address the items that apply to them. The FTC Compliance Guide provides a helpful example in explaining this point. If a financial institution doesn't share NPI with affiliates or nonaffiliated third parties, the financial institution can provide a simplified notice that:

1) Describes their collection of NPI;
2) States that the financial institution only discloses NPI to nonaffiliated third parties "as permitted by law;" and
3) Explains how the financial institution protects the confidentiality and security of NPI.

Privacy Notice to Customers. There are several unique obligations to consumers. First, Financial institutions must provide all customers with an initial privacy notice, whether or not they share customer NPI.[111] The initial notice must be provided by the time the customer relationship is established[112] and must include:

1) An "opt-out" notice explaining the individual's right to direct the financial institution not to share their NPI with a nonaffiliated third party;
2) A reasonable way to opt out;
3) A reasonable amount of time to opt out before disclosing the NPI.

Financial institutions must additionally provide customers with an "annual notice" which includes a copy of the complete privacy notice.[113] The financial institution must additional provide a new opt out notice and give the consumer a reasonable opportunity to opt out of the disclosure.[114]

Further, while generally new privacy notices are not required for each new product or service, a financial institution must provide a new notice to an *existing* customer when that customer obtains a new financial product/service from

[109] § 313.6(c)(1)(i)-(iv).
[110] § 313.6(a)(1)-(9).
[111] § 313.4(a).
[112] § 313.4(a)(1).
[113] *See generally* § 313.5.
[114] § 313.8(a)(2),(3).

the institution IF the initial notice or annual notice most recently provided to the customer was not accurate with respect to the new financial service/product.[115]

Privacy Notices to Consumers Who Are Not Customers. Financial Institutions must provide a privacy notice to consumers only if they share NPI with nonaffiliated third parties.[116] If they do intend to share NPI with nonaffiliated third parties, the financial institution must provide to the consumer:

1) An initial notice of its privacy policies;
2) An opt out notice (including a reasonable means to opt out);
3) A reasonable opportunity to opt out.[117]

Instead of a full privacy notice, consumers may be provided a "short-form" notice which must contain:

1) That the full privacy notice is available upon request;
2) Describe a reasonable way consumers may get the full privacy notice;
3) Include an opt-out notice[118]

The Safeguards Rule

In short, the Safeguards Rule requires financial institutions to "develop, implement, and maintain, and information security program with administrative, technical, and physical safeguards designed to protect customer information."[119] The Safeguards Rule took effect in 2003 and was subsequently amended in 2021 due to developments in technology. Information security programs must be written, and be appropriate based on:

1) The size and complexity of the organization and its operation
2) The nature and scope of the institution's activities involving consumer information
3) The sensitivity of the customer information the institution handles[120]

Under 16 C.F.R. § 314.4 – 314.6, the Safeguard Rule stipulates that, in order to develop, implement, and maintain the information security program, businesses shall:

1) Designate a qualified individual to oversee, implement, and enforce the information security program.[121]
2) Conduct a risk assessment related to both external and internal risks.
3) Design and implement safeguards to control the risks identified through the risk assessment.
4) Regularly monitor and test the effectiveness of the safeguards.
5) Appropriately train staff.
6) Monitor service providers
7) Keep the information program current.
8) Create a written incident response plan in response to any security event.[122]
9) Require the qualified information to report to the board of directors.

---

[115] § 313.4(d)(1),(2).
[116] § 313.4(b).
[117] § 313.7.
[118] §§ 313.6(d)(1),(2).
[119] Federal Trade Commission, *FTC Safeguards Rule: What Your Business Needs to Know*, Business Guidance, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know; § 314.2(j) ("Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.").
[120] § 314.3(a).
[121] § 314.4(a).
[122] § 314.4(h) (stipulating what must be included in the incident response plan); § 314.2(p) ("Security event means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form").

Pretexting Provisions

This provision of the GLBA prohibits the practice of pretexting or accessing private information using false pretenses. While the GLBA does not have specific requirements regarding pretexting, prevention usually entails building employee training to avoid pretexting scenarios.

Enforcement

The Dodd-Frank Act transferred rulemaking authority to the Bureau of Consumer Financial Protection (with some exceptions), however, the Federal Trade Commission maintains enforcement authority.

For More Information:

- Text of the Act, here and here
- Federal Trade Commission, Gramm-Leach-Bliley Act
- Federal Trade Commission, FTC Safeguards Rule: What Your Business Needs to Know
- U.S. Department of Education, Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements
- Federal Deposit Insurance Corporation, Privacy of Consumer Financial Information
- International Association of Privacy Professionals, Guide to the Gramm-Leach-Bliley Act
- Federal Trade Commission, Legal Library: Cases and Proceedings Concerning GLBA

Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed The Health Insurance Portability and Accountability Act of 1996 which at its foundation, focused on "portability" or the idea that individuals could "take" their health insurance coverage between employers, without pre-existing health conditions serving as an impediment to job transitions.[123] In 2003, the HHS issued the HIPAA privacy rule to assure that individual's health information is properly protected while allowing the flow of information needed to provide and promote high quality health care.[124]

HIPAA AT A GLANCE

Regulates: Health Care Providers, Health Insurance, Health Care Clearinghouse
Mission: Consumer Protection
Law: Codified in relevant part primarily at 15 U.S.C. §§ 6801-6809, §§ 6821-6827. Pub. L. 104-191

HIPAA is a very long and complicated statute, and this section does not attempt to summarize the entire regulation. Rather, this section will focus on the provisions of HIPAA that relate to information privacy.

HIPAA consists of five titles:

Title I: Health Care Access, Portability, and Renewability

Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform

Title III: Tax Related Health Provisions Governing Medical Savings Accounts

Title IV: Application and Enforcement of Group Health Insurance Requirements

Title V: Revenue Offset Governing Tax Deductions for Employers

This section will discuss the Privacy Rule and the Security Rule, both of which fall under Title II.

The Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' health information (Personal Health Information or PHI) by entities subject to the Privacy Rule.[125] First, how does HIPAA approach Personal Health Information? There are two important definitions to understand. First, 45 C.F.R. § 160.103 defines individually identifiable information as

> information that is a subset of health information, including demographic information collected from an individual, and:
>
> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> > (i) That identifies the individual; or
> >
> > (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

[123] *HIPAA Privacy and Security for Beginners*, Wiley Rein (Jul. 2014) https://www.wiley.law/newsletter-5029
[124] *Id.*
[125] *The HIPAA Privacy Rule*, Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

From there, this section defines *Protected Health Information* as: individually identifiable health information . . .

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

To make clear, Personal Health Information is not all health information about an individual. Rather, it is certain information that is protected when it is held or created by certain entities for certain purposes. There are no restrictions on the use or disclosure of de-identified health information. Once the information has been de-identified, then it is no longer "individually identifiable" and no longer covered. The Privacy Rule provides two de-identification methods, Expert Determination or Safe Harbor:

1) A formal determination by a qualified expert; or
2) The removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual[126]

Next, what entities are regulated by HIPAA? HIPAA directly regulates what it refers to as "covered entities," which includes:

Healthcare Providers	Health Plans	Health Care Clearinghouses
regardless of size of practice, who electronically transmit health information in connection with *certain transactions*. These transactions include: 1. Claims 2. Benefit eligibility requirements 3. Referral authorization requests 4. Other transactions for which HHS has established standards under the HIPAA Transactions Rule.	1. Health, dental, vision, and prescription drug insurers 2. Health maintenance organizations (HMOs) 3. Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers 4. Long-term care insurers (excluding nursing home fixed-indemnity policies) 5. Employer-sponsored group health plans 6. Government – and church – sponsored health plans 7. Multi-employer health plans	or entities that process nonstandard information they receive from another entity into a standard, or vice versa. This category includes: 1. billing services 2. repricing companies 3. community health management information systems 4. and value-added networks and switches if these entities perform clearinghouse functions.

[126] For more information on de-identification in accordance with the HIPAA Privacy Rule, *see* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale

Additionally, **Business Associates** are an entity indirectly regulated by HIPAA and are

> a person who, on behalf of *covered entities*, creates, receives, maintains, or transmits PHI for a function or activity including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or (2) Provides, . . . legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.[127]

The Privacy Rule imposes an obligation on covered entities to have a contract, or a standard business associate agreement, with their business associates.[128] As such, business associates have contractual obligations to apply privacy and security controls in line with HIPAA requirements. In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.[129] Further, a covered entity *may not* contractually authorize its business associate to make any use or disclosure of PHI that would violate the Rule.[130]

As a result of the 2009 "HITECH" law and 2013 HHS regulations, "business associates" must comply directly with significant portions of the HIPAA rules.[131] Further, the HITECH regulations extended the business associate compliance obligations "downstream" to service providers of a business associate, and service providers to that downstream associate, and so on.[132] These subcontractors face the same compliance obligations as a first tier business associate that contracts directly will a covered entity.[133]

Use and Disclosure Under The Privacy Rule

The general principle behind HIPAA's use and disclosure rules are fairly simple and can be found at 45 C.F.R. Part 160 and Part 164, subparts A and E.[134] Generally, the Rule "prohibits a covered entity from using or disclosing protected health information unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities."[135]

Permitted Use and Disclosures - There are a few permitted uses and disclosures that HIPAA treats as necessary to the basic function of the healthcare system.[136] Specifically, covered entities are permitted, but not required, to use and disclose PHI, without an individual's authorization, for the following purposes:

(1) To the Individual. Covered entities may disclose PHI to the individual who is the subject of the information.[137]

---

[127] §§ 164.502(e), 164.504(e), 164.532(d),(e).
[128] § 164.504(e)(1).
[129] § 164.504(e)(2)(i).
[130] *Id.*
[131] *Direct Liability of Business Associates*, Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html
[132] Jonathan P. Tomes, *Avoiding Liability for Business Associates' Breaches: Adjustments and Ongoing Strategies*, American Health Information Management Association (AHIMA), https://bok.ahima.org/doc?oid=300875#.ZEwwfHbMLMZ.
[133] *Id.*
[134] 45 C.F.R. 160 Subpart A "General Provisions"; 45 C.F.R. 164 Subparts A, E.
[135] Health and Human Services, *Use and Disclosures for Treatment, Payment, and Health Care Operations*, Guidance Materials, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html
[136] § 164.506(a); *see* § 164.501 "Definitions".
[137]

(2) "TPO" or Treatment, Payment, and Health Care Operations.[138]

- ***Treatment*** means the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[139]
- ***Payment*** involves the activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and to provide reimbursement for the provision of healthcare.[140] These activities relate to the individual to whom health care is provided, but 45 C.F.R. § 164.501 at Payment, paragraph 2 contain some covered scenarios.
- ***Health Care Operations*** mean any of the following activities to the extent that they are related to covered functions: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[141]

(3) Uses and Disclosures with Opportunity to Agree or Object.[142] Under 45 C.F.R. § 164.510(a), a covered entity may use/disclose PHI, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree, prohibit, or restrict the use or disclosure. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

- ***Facility Directories***. If the facility maintains a facility directory, it may use or disclose limited information about the patient, after giving the individual an opportunity to agree or object. The categories of PHI may be used to maintain the directory are listed under § 164.510(a)(i)(A)-(D).
- ***Notification and Other Purposes.*** Covered entities may disclose PHI to a family member, other relative, close personal friend of the patient, or any other person identified by the patient who is involved with the patient's health care or payment.[143] Similarly, a covered entity may rely on an individual's informal permission to use/disclose PHI for the purpose of notifying (including identifying or locating) family members, personal representations, or others responsible for the individual's care of the individual's location, general condition, or death.[144] Additionally, PHI may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.[145]

(4) Incident to an Otherwise Permitted Use and Disclosure. The Privacy Rule does not require that *every single risk* of an incidental use/disclosure of PHI be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards and the information being shared was limited to the "minimum necessary."[146]

---

[138] § 164.501.
[139] *Id.* at "Treatment".
[140] *Id* at "Payment"(1).
[141] § 164.501 at "Health Care Operations"
[142] § 164.510.
[143] § 164.510(b)(1).
[144] § 164.510(b)(1)(ii).
[145] § 164.510(b)(4); *see also* § 164.512(b)(1)(i) (permitting covered entities to, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority).
[146] 45 C.F.R. §§ 164.502(a)(1)(iii).

(5) Public Interest and Benefit Activities. The Privacy Rule permits use/disclosure of PHI, without an individual's authorization or permission, for 12 national security purposes.[147] These are permitted, not required, disclosures. There are specific conditions or limitations applicable to each public interest purpose to balance the individual privacy interest.

- ***Required by Law***. Includes legal requirements by statute, regulation, or court orders.[148]
- ***Public Health Activities***. Covered entities may disclose PHI to: (1) Public Health Authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability;"[149] (2) entities subject to FDA regulation regarding FDA regulated products/activities for purposes such as adverse event reporting or product recalls; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information regarding a work-related illness or injury because such information is needed by the employer in order to comply with OHSA, MHSA, or a similar law.[150]
- ***Victims of Abuse, Neglect, or Domestic Violence***. In certain circumstances, covered entities may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[151]
- ***Health Oversight Activities***. Covered entities may disclose protected health information to health oversight agencies for purposes of legally authorized health oversight activities, such as investigations necessary for government benefit programs.[152]
- ***Judicial and Administrative Proceedings***. May disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal or, depending on assurances, a subpoena.[153]
- ***Law Enforcement Purposes***.[154] Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under six circumstances, and subject to specified conditions:
    1. as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
    2. to identify or locate a suspect, fugitive, material witness, or missing person;
    3. in response to a law enforcement official's request for information about a victim or suspected victim of a crime;
    4. to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
    5. when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and
    6. by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.
- ***Decedents***. Disclosures of PHI to funeral directors as needed, to coroners or medical examiners for the purpose of identifying a deceased person, determining the cause of death, and performing other functions authorized by law.[155]
- ***Cadaveric Organ, Eye, or Tissue Donation***. Disclosures to facilitate the donation and transplantation of cadaveric organs, eyes, and tissues.[156]
- ***Research***.[157] Use and disclosure of PHI for research purposes, provided the covered entity obtains either:

---

[147] *See* § 164.512.
[148] § 164.512(a).
[149] Health and Human Services *supra* note 64; *see* 45 C.F.R. § 164.512(b)(1)(i);
[150] § 164.512(b).
[151] § 164.512(a), (c).
[152] § 164.512(d).
[153] § 164.512(e).
[154] § 164.512(f).
[155] § 164.512(f).
[156] § 164.512(g).
[157] § 164.512(h); § 164.501 ("'Research' is any systematic investigation designed to develop or contribute to generalizable knowledge").

1. Documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;
2. Representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or
3. Representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.

- ***Serious Threat to Health and Safety***. Disclosures of PHI necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat.[158]
- ***Essential Government Functions***. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.[159]
- ***Worker's Compensation***. Disclosures in order to comply with workers' compensation laws and other similar programs.[160]

(6) Limited Data Set. A limited data set is PHI from which certain direct identifiers of individuals and their relatives, household members, and employers have been removed. May be used/disclosed for research, health care operations, and public health purposes.[161]

Authorized Uses and Disclosures. First, what is an authorization? An authorization must be written in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization, or by a third party. All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.[162]

Psychotherapy Notes. Covered entities must obtain an individual's authorization to use/disclose psychotherapy notes, though there are two exceptions under 45 C.F.R. § 164.508(a)(2).[163]

Marketing. The ability for covered entities to use PHI for the purposes of marketing is very limited. Marketing is defined as making a communication that encourages the recipient to use a product or service, with certain excepted activities that relate to an individual's specific treatment or the operations of a provider or plan to provide general information about case management and other services.[164]

A covered entity must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;
- Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;

---

158 § 164.512(j).
159 § 164.512(k).
160 § 164.512(l).
161 § 164.514(e); § 164.514(e)(2) (defining limited data set).
162 *See* § 164.508(b)(1).
163 § 164.508(a)(2).
164 §§ 164.501, 164.508(a)(3).

- Communications for treatment of the individuals; and
- Communications for case management or care coordination for the individual.[165]

If the marketing involved financial renumeration to the covered entity from a third party, the authorization must state that such renumeration is involved.[166]

Individual Rights

These rules and others work together to provide individuals with specific individual rights, they are specifically detailed in 45 C.F.R. 164.520(b)(1)(iv).

1. The right to request restrictions on certain uses and disclosures of PHI as provided by § 164.522(a);
2. The right to receive confidential communications of PHI as provided by § 164.522(b);
3. The right to inspect and copy PHI as provided by § 164.526;
4. The right to amend PHI as provided by § 164.526;
5. The right to receive an accounting of disclosures of PHI as provided by § 164.528; and
6. The right of an individual, including an individual who has agreed to receive the notice electronically, to obtain a paper copy of the notice.

The Privacy Notice

Health care providers and health plans must provide privacy notices detailing how they may use and share health information. The privacy notice must be written in plain language and contain certain elements:

1. The following statement as a header or otherwise prominently displayed:
   "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

2. Certain information regarding uses and disclosures:
   - A description (and at least one example) of the types of uses and disclosures that the covered entity is permitted by this subpart to make for the purposes of treatment, payment, and healthcare operations.
   - A description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information without the individual's written authorization.
   - A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization.
3. Separate statements for certain uses or disclosures:
   - The covered entity may contact the individual to raise funds for the covered entity and the individual has the right to opt out of receiving such communications;
   - The group heath plan may disclose PHI to the sponsor of the plan; or
   - If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.
4. The individual rights listed in the prior section of this Memo, and a brief description of how the individual may exercise these rights.
5. The following information regarding the covered entity's duties:
   - A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices

[165] § 164.501.

[166] § 164.508(a)(3)(ii); § 164.501 (Financial remuneration means direct or indirect payment that flows from or on behalf of a third party whose product or service is being described and does not include payment for the treatment of an individual.).

with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;
    - A statement that the covered entity is required to abide by the terms of the notice currently in effect; and
    - For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains.
6. A statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, as well as a description of how they may file a complaint, and an assurance that the individual will not be retaliated against for filing a complaint.
7. The name, or title, and telephone number of a person or office to contact for further information.

45 C.F.R. § 164.520(c) provides additional information on how and when different covered entities must provide notice.

The Security Rule

The Security Rule "requires physicians to protect patients' electronically stored, protected health information (known as "ePHI") by using appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of this information."[167] The rule can be found at 45 C.F.R. Part 160 and subparts A and C of Part 164. Section 164.306 outlines the general requirements of covered entities and business associates:

- Ensure the confidentiality,[168] integrity,[169] and availability[170] of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required subpart E of Part 164;
- Ensure compliance with this subpart by its workforce[171]

HIPAA does not require a specific security measure in order to implement the above standards, but requires that a covered entity or business associate take into account the following factors when creating their security measures:

- The size, complexity, and capabilities of the covered entity or business associate
- The covered entity's or business associate's technical infrastructure, hardware, software security capabilities;
- The costs of security measures;

[167] American Medical Association, *HIPAA Security Rule & Risk Analysis*, Practice Management, https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis#:~:text=The%20HIPAA%20Security%20Rule%20requires,and%20security%20of%20this%20information.
[168] § 164.304 "Confidentiality" (Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes).
[169] § 164.304 "Integrity" (Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner).
[170] § 164.304 "Availability" (Authentication means the property that data or information is accessible and useable upon demand by an authorized person.).
[171] § 164.306(a)(1)-(4).

- The probability and criticality of potential risks to electronic protected health information.[172]

The Security Rule has 18 safeguards standards, each of which is mandatory, in addition to 36 implementation specifications.[173] Implementations are either "required" (must be implemented) or "addressable" (may be replaced with reasonable and appropriate alternatives).[174] Of note, addressable implementation specifications are NOT optional. The Rule is split into Administrative Safeguards,[175] Physical Safeguards, Technical Safeguards – we will discuss each briefly.

Administrative Safeguards:

1. Security Management Process: implement policies and procedures to prevent, detect, contain, and correct security violations.[176]
    a. Risk Analysis (Required)
    b. Risk Management (Required)
    c. Sanctions Policy (Required)
    d. Information Systems Activity Review (Required)[177]

2. Assigned Security Responsibility: Identify a Security Official who is responsible for the development and implementation of the security management process.[178]

3. Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information.[179]
    a. Authorization and Supervision (Addressable)
    b. Workforce Clearance Procedure (Addressable)
    c. Termination Procedures (Addressable)[180]

4. Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information.[181]
    a. Isolation of Healthcare Clearinghouse Functions (Required)
    b. Access Authorization (Addressable)
    c. Access Establishment and Modification (Addressable)[182]

5. Security Awareness and Training: Implement a security awareness and training program for all employees, including management.[183]
    a. Security Reminders (Addressable)
    b. Protection from Malicious Software (Addressable)
    c. Login Monitoring (Addressable)
    d. Password Management (Addressable)[184]

6. Security Incident Procedures: Implement policies and procedures to address security incidents.[185]
    a. Response and Reporting (Required)[186]

---

[172] § 164.306(b)(2)(i)-(iv).
[173] Daniel J. Solove, *HIPAA Security Rule Checklist*, Teach Privacy, https://teachprivacy.com/hipaa-security-rule-checklist-5/; Implementation specification
[174] *Id.*; 45 C.F.R. 164.306(d)(3)(ii)(B).
[175] § 164.308.
[176] § 164.308(a)(1)(i).
[177] § 164.308(a)(1)(ii)(A)-(D).
[178] § 164.308(a)(2).
[179] § 164.308(a)(3)(i).
[180] § 164.308(a)(3)(ii)(A)-(C).
[181] § 164.308(a)(4)(i).
[182] § 164.308(a)(4)(ii)(A)-(C).
[183] § 164.308(a)(5)(i).
[184] § 164.308(a)(5)(ii)(A)-(D).
[185] § 164.308(a)(6)(i).
[186] § 164.308(a)(6)(ii).

7. Contingency Plan: Establish policies and procedures for responding to an emergency occurrence that damages systems that contain ePHI
    a. Data Backup Plan (Required)
    b. Disaster Recovery Plan (Required)
    c. Emergency Mode Operations Plan (Required)
    d. Testing and Revision Procedures (Addressable)
    e. Applications and Data Criticality Analysis (Addressable)[187]

8. Evaluation: Routinely evaluate the implementation of the administrative, physical, and technical safeguards.[188]

9. Business Associate Contracts and Other Arrangements: Business Associate must make an agreement ensuring to implement their own procedures to reach compliance with the Security Rule.[189]
    a. Written Contract or Other Arrangement (Required)[190]

Physical Safeguards:

1. Facility Access Controls: Implement policies and procedures to limit access to the computer systems which contain ePHI.[191]
    a. Contingency Operations (Addressable)
    b. Facility Security Plan (Addressable)
    c. Access Control and Validation Procedures (Addressable)
    d. Maintenance Records (Addressable)[192]

2. Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.[193]
3. Workstation Security: Implement physical safeguards for all workstations to restrict access to ePHI to authorized users.[194]
4. Device and Media Controls: Manage hardware and electronic media containing ePHI to restrict access to authorized users.[195]
    a. Disposal (Required)
    b. Media Reuse (Required)
    c. Accountability (Addressable)
    d. Data Backup and Storage (Addressable)[196]

Technical Safeguards:

1. Access Control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to authorized users.[197]
    a. Unique User Identification (Required)
    b. Emergency Access Procedure (Required)
    c. Automatic Log-off (Addressable)
    d. Encryption and Decryption (Addressable)[198]

---

[187] § 164.308(a)(7)(ii)(A)-(E).
[188] § 164.308(a)(8).
[189] § 164.308(b)(1).
[190] § 164.308(b)(3).
[191] § 164.310(a)(1).
[192] § 164.310(a)(2)(i)-(iv).
[193] § 164.310(b).
[194] § 164.310(b).
[195] § 164.310(d)(1).
[196] § 164.310(d)(2)(iv).
[197] § 164.312(a)(1).
[198] § 164.312(a)(2)(i)-(iv); *see also* § 164.304 "Encryption" (Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.).

2. Audit Controls: Implement hardware/software/procedural mechanisms that record and examine activity in information systems that contain/use ePHI.[199]

3. Integrity: Implement policies/procedures to protect ePHI from improper alteration or destruction.[200]
    a. Mechanism to Authenticate ePHI (Addressable)[201]

4. Person or Entity Authentication: Implement procedures to verify that a person seeking access to ePHI is the one claimed.[202]

5. Transmission Security: Implement technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network.[203]
    a. Integrity Controls (Addressable)
    b. Encryption (Addressable)

Enforcement

HIPAA's Privacy and Security Rules are enforced by the Health and Human Services' Office for Civil Rights.[204] The HIPAA Enforcement Rule is codified at 45 C.F.R. Part 160, Subparts C, D, and E.

For More Information:

- Combined Text of the Privacy Rule
- Health and Human Services, Summary of the HIPAA Privacy Rule
- Center for Medicare and Medicaid Services, HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules
- Health and Human Services, Your Rights Under HIPAA
- Health and Human Services, Guidance on Treatment, Payment, & Health Care Operations
- File a Complaint
- Health and Human Services, Individuals Right under HIPAA to Access their Health Information

[199] § 164.312(b).
[200] § 164.312(c)(1).
[201] § 164.312(c)(2).
[202] § 164.312(d).
[203] § 164.312(e)(1).
[204] *HIPAA Enforcement,* Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

Section 5 of the FTC Act

The FTC Act grants the Commission authority to enforce fair competition law. [205] Most enforcement authority derives from Section 5 of the FTC Act, which has a two prong approach. The first prong addresses consumer protection, while the second prong addresses primarily antitrust.[206] The first prong will be the focus of this section.

§5, FTC ACT AT A GLANCE

Regulates: All persons engaged in commerce
Mission: Consumer Protection
Law: 15 U.S.C. § 45

Under Section 5, the FTC prohibits unfair or deceptive acts or practices in or affecting commerce.[207] This is the most common enforcement mechanism in the privacy arena. The prohibition applies to all persons engaged in commerce, including banks, though banking agencies[208] have authority to enforce §5 for the institutions they supervise, and their institution affiliated parties (IAP).[209] The legal standards, *unfairness* and *deception* are independent of each other. An act may be unfair but not deceptive, deceptive but not unfair, or both.

An act or practice is *unfair* where it:

1. Causes or is likely to cause substantial injury to consumers,
2. Cannot be reasonably avoided by consumers, and
3. Is not outweighed by countervailing benefits to consumers or competition.[210]

An act or practice is *deceptive* if is it includes:

1. A material misrepresentation, omission OR practice;
2. That is likely to mislead a consumer acting reasonably.[211]

When determining whether an act or practice may be considered unfair or deceptive, they may additionally take into account public policy, whether established by statute, regulation, or judicial decisions.

This provision grants the FTC wide enforcement authority in consumer protection. Additionally, under the U.S. Safe Web Act, "unfair or deceptive acts or practices" include such acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States, OR involve material conduct occurring within the U.S.[212]

For More Information:

- Federal Trade Commission, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act
- Daniel Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy
- Cobun Zweifel, White Paper: IAPP Guide to FTC Privacy Enforcement

[205] Pub. L. No. 63-203, 38 Stat. 717; 15 U.S.C. § 45(a)(1)
[206] 15 U.S.C. §1681s(a),(b).
[207] 15 U.S.C. §1681s(a)(1).
[208] Federal Deposit Insurance Company, Federal Reserve Board, and Office of the Comptroller of the Currency.
[209] Federal Deposit Insurance Corporation, *VII. Unfair, Deceptive, and Abusive Practices – Federal Trade Commission Act/Dodd-Frank Act*, FDIC Consumer Compliance Examination Manual (Jun. 2022) https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-1-1.pdf.
[210] 15 U.S.C. § 45(n).
[211] *Id.*
[212] 15 U.S.C. § 45(a)(4)(A).

State Level Privacy Regulations

There are few states that have enacted comprehensive privacy laws, though many may have privacy laws which regulate certain kinds of information, such as Illinois' Biometric Information Privacy Act (BIPA). This memo will not discuss each privacy law in each state, but will cover a handful of comprehensive privacy laws, as well as BIPA.

Resources on State Privacy Laws, Generally:

- International Association of Privacy Professionals, Building a Comprehensive Program for a Patchwork of State Privacy Laws
- IAPP, US State Privacy Legislation Tracker
- Bloomberg Law, Data Privacy Laws: CA vs VA Comparison Chart
- Husch Blackwell, *A Comprehensive Resource for Tracking U.S. State Biometric Privacy Legislation*

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act is legislation designed to strengthen privacy rights for California residents.[213] In essence, CCPA is an "opt-out" privacy regulation which gives citizens the right to access, delete, and opt out of sharing or selling their personal information.[214] The law provides expansive rights to Californians and is intended to be liberally construed to effectuate the purpose of the law.[215] There are also new obligations for covered businesses when updating their privacy programs.[216] CCPA was amended by the California Privacy Rights Act (CCPA) in 2018; the following is a discussion of the CCPA as amended by the CPRA, and accounts for amendments up to January 1, 2023.[217]

In a nutshell, the CCPA grants rights to consumers and places restrictions and obligations on covered businesses. So first, which businesses are covered? CCPA applies to businesses that collect[218] and control California residents' personal information, do business in the state of California, AND

- Have an annual gross revenue in excess of $25 Million in the preceding calendar year; or
- Annually buys, sells, or shares the personal information of 100k consumers[219] or households; or
- Derives 50% or more of their annual revenues from selling California residents' personal information.[220]

However, businesses that are already subject to federal data protection regulations are exempted under CCPA.[221] These include:

- Health providers and insurers subject to HIPAA
- Banks and financial companies covered by Gramm-Leach-Bliley
- Credit reporting agencies that are covered by the Fair Credit Reporting Act

[213] Cal. Civ. Code § 1798.100 et seq. (2018)
[214] Christina De Jong, et al., *A Quick Reference Guide for CCPA Compliance*, Deloitte, https://www2.deloitte.com/us/en/pages/advisory/articles/ccpa-compliance-readiness.html
[215] Cal. Code Title 1.81.5. § 1798.194.
[216] *Id.*
[217] *See California Consumer Privacy Act (CCPA)*, Office of the Attorney General (Feb. 15 2023) https://oag.ca.gov/privacy/ccpa.
[218] *See* §1798.140(f) (defining "collects," "collected," or "collection.").
[219] §1798.140(i) (defining "consumer.")
[220] Cal. Code Title 1.81.5. §1798.140(d)(1).
[221]

Next, what type of information is protected? The Act protects certain information defined as personal information, or:

> . . .[I]nformation that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.[222]

Personal information includes, but is not limited to, the following *if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonable linked, directly or indirectly, with a particular consumer or household:*

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories;
- Biometric information;[223]
- Internet or other electronic network activity information, including browsing history and search history;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education Information defined under FERPA;[224]
- Inferences drawn from any of the information identified in that subdivision of the act to "create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Sensitive personal information

There are three exceptions to the definition of personal information. First, personal information does not include *publicly available information*, or, information that is lawfully available from federal, state, or local governments.[225] Biometric information is not considered to fall under "publicly available information" if it was collected by a business without a consumer's knowledge.[226] Additionally, personal information does not include consumer information that is de identified or consumer information that is aggregated.[227]

The CPA provides for a subcategory of personal information: sensitive personal information.[228] Sensitive personal information is personal information that reveals:

- A consumer's social security, driver's license, state identification card, or passport number;

---

[222] Cal. Code Title 1.81.5. §1798.140(v)(1).

[223] Cal. Code Title 1.81.5 § 1798.140(c) ("'Biometric Information' means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.").

[224] *See* 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

[225] Cal. Code Title 1.81.5. §1798.140(v)(2).

[226] *Id.*

[227] §§ 1798.140(v)(3); 1798.140(a) ("Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device"); §1798.140(m) ("Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification. . . (2) has implemented business processes that specifically prohibit reidentification. . .(3) Has implemented business processes to prevent inadvertent release. . .(4) Makes no attempt to reidentify the information.").

[228] § 1798.140(ae)(1).

- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- Precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;
- A consumer's genetic data

Sensitive personal information also includes the processing of biometric information for the purpose of uniquely identifying a consumer, such as personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.[229]

Individual Rights

The CCPA established an expansive list of consumer individual rights. Briefly, those are as follows:

The Right to Delete. Also known as "the right to be forgotten", consumers have the right to request that businesses delete personal information they collected from the consumer, and to request that service providers do the same.[230] However, § 1798.105(d) contains explicit exemptions on when a business is not required to delete the consumer's information.[231]

The Right to Correction. Consumers may request that businesses correct inaccurate information that the business has about them.[232] Section 1798.185(a)(8) contains guidance on how often, and under what circumstances, a consumer may request a correction.[233]

The Right to Notice. A business must, at or before the point of collection, inform consumers about the categories of personal information to be collected, as well as the purposes for which the categories of personal information shall be used.[234] Businesses must provide notice again before collecting additional categories or collecting personal information for new purposes.[235] Additionally, businesses must notify consumers of their rights under CCPA.[236]

The Right to Know and Access. Consumers have the right to request that businesses disclose what information they collect on a consumer, specifically businesses must disclose:

- The categories of PI it has collected;
- The categories of sources from which the PI is collected;
- The business of commercial purpose for collected, selling, or sharing PI;
- The categories of third parties to whom the business discloses PI; and
- The specific pieces of PI it has collected about that consumer.[237]

Californians can make a free request up to twice a year, and the information provided must cover the 12 month period prior to the request.[238] The information must be provided to the consumer in a format that is easily

[229] § 1798.140(ae)(2).
[230] §§ 1798.105(a),(c).
[231] § 1798.105(d)(1)-(8).
[232] § 1798.106(A).
[233] § 1798.185(a)(8)(A)-(D).
[234] § 1798.100(b).
[235] *Id.*
[236] §§ 1798.105(b), 1798.106(b), 1798.110(c), 1798.115(c), 1798.120(b), 1798.121(b), 1798.130.
[237] § 1798.110(a)(1)-(5).
[238] § 1798.130(2)(A).

understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity easily.[239]

Consumers additionally have the right to request that a business that sells, shares, or discloses a consumer's PI, disclose to the consumer:

1. The categories of personal information that the business collected about the consumer;
2. The categories of personal information that the business sold or shared, and the categories of third parties to whom the information was sold or shared; and
3. The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed.[240]

The Right to Opt-Out of Sale or Sharing. Consumers may, at any time, request that businesses stop selling their personal data and must wait at least 12 months before asking consumers to opt back in.[241] A business is not permitted to sell the personal information of consumers if the business has *actual knowledge* that the consumer is less than 16.[242] However, if the business receives affirmative authorization ("opt-in"), the business may sell that personal information.[243] For children under 13, parental consent is required. For children who are at least 13 but under 16, the child can opt-in themselves.[244]

Right to Limit Sensitive Personal Information. Consumers have the right to direct businesses to restrict the use of their sensitive personal information for limited purposes, such as providing the requested service.[245] However, sensitive PI that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section.[246]

The Right to Non-Discrimination. This provision intends to protect consumers from retaliation when they exercise their rights under CCPA.[247] Specifically, a business may not discriminate against a consumer by:

- Denying goods or services to the consumer
- Charging different prices or rates for goods or services, regardless of whether or not that would be accomplished through discounts or imposing penalties[248]
- Providing a different level or quality of goods
- Suggesting that the consumer will receive a different price or different quality of goods or services.[249]

This provision does not prohibit a business from offering loyalty, rewards, premium features, discounts or club card programs.[250]

Before covering more obligations imposed on businesses, what does it mean for a consumer to consent to the use or disclosure of their personal information? Under CCPA, consent must be freely given, specific, informed, and unambiguous.[251] The Rule additionally provides examples of practices that do *not* constitute consent. Those are:

---

[239] § 1798.130(a)(d)(B)(iii).
[240] § 1798.115(a)(1)-(3).
[241] §§ 1798.120(a); 1798.135(c)(4).
[242] § 1798.120(c).
[243] *Id.*
[244] *Id.*
[245] § 1798.121(a); *see* § 1798.140(ae) (defining "sensitive personal information").
[246] § 1798.121(d).
[247] § 1798.125.
[248] § 1798.125(a)(1)(A)-(D).
[249] § 1798.125(a)(1)(A)-(D).
[250] § 1798.125(a)(3).
[251] § 1798.140(h).

- Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information.
- Hovering over, muting, pausing, or closing a given piece of content.
- Agreement obtained through use of dark patterns.[252]

Responsibilities on Businesses

Notice, Disclosure, Correction, and Deletion Requirements

Businesses must offer two or more methods for consumers to submit the requests associated with the above rights and, at minimum, include a toll-free telephone number.[253] Businesses that operate exclusively online and have a direct relationship with a consumer are only required to provide an email address for submitting requests.[254] If a business operates an internet website, the website should be available to consumers to submit requests as well.[255]

Businesses must make the requested disclosures within 45 days of receiving a verifiable consumer request.[256] The business may, only once, request an additional 45 days where reasonably necessary, so long as the consumer is provided notice within the first 45 days.[257]

Additionally, businesses that sell personal information must provide a clear and conspicuous "Do Not Sell My Personal Information" link on their website where consumers may submit an opt-out request.[258] Consumers cannot be required to make an account to opt out nor should the business require consumers to verify their identity outside of questions necessary to identify which personal information belongs to the consumer.[259]

The Privacy Notice.

In addition to the point of collection notices, businesses must disclose certain information in its online policy or policies or on its internet website.[260] The posted privacy notice must be updated annually and contain a description of a consumer's rights under CCPA and two or more designated methods for submitting requests. Further, the privacy notice must contain:

- A list of the categories of PI it has collected about consumers in the preceding 12 months;
- The categories of sources from which consumers' personal information is collected;
- The business or commercial purpose for collecting, selling, or sharing consumers' PI;

Further, the privacy policy must contain two separate lists with:

- The categories of personal information the business has sold or shared about consumers in the preceding 12 months; and

[252] *Id.*; *see also* Catherine Zhu, *Dark Patterns – a New Frontier in Privacy Regulation*, Reuters (Jul. 29, 2021) https://www.reuters.com/legal/legalindustry/dark-patterns-new-frontier-privacy-regulation-2021-07-29/ ("Dark patterns are manipulative or deceptive practices built into user interfaces by developers that have the effect, intentionally or unintentionally, of obscuring, subverting, or impairing consumer autonomy, decision-making, or choice.").
[253] § 1798.130(a)(1)(A).
[254] *Id.*
[255] § 1798.130(a)(1)(B).
[256] § 1798.130(a)(2)(A).
[257] *Id.*
[258] § 1798.135(a)(1).
[259] § 1798.100(d).
[260] § 1789.130(a)(5)(B).

- A list of the categories of PI the business has disclosed about consumers for a business purpose in the preceding 12 months.[261]

A third party that controls the collection of PI may satisfy its notice obligation by providing the above required information prominently and conspicuously on the home page of its internet website.[262] If the business controls the collection of PI about a consumer on its premises, the business must, at or before the point of collection, the same three categories listed above.[263]

Further, a business' collection, use, retention, and sharing of a consumer's PI must be **reasonably necessary and proportionate** to achieve the purpose for which the information was collected in the first place.[264]

Covered businesses that sell or share PI with a third party, or that discloses PI to a service provider or contractor for a business purpose, must enter into a specific agreement with that third party.[265] The agreement must:

1. Specify that the PI is sold or disclosed by the business only for a limited and specified purpose
2. Obligate the third party to comply with applicable obligations under CCPA, and obligates those third parties to provide the same level of privacy protection that is required of the business under CCPA.
3. Require the third party to notify the business if it can no longer meet its obligations.
4. Grant the business the right to take reasonable and appropriate steps to top and remediate the unauthorized use of PI.

Businesses must additionally include a clear and conspicuous "Do Not Sell or Share Link" in the notice at collection to enable consumers to opt-out of the sale or sharing of their PI.[266] Businesses must additional provide a clear and conspicuous link on the business's homepage "Limit the Use of My Sensitive Personal Information" that enables the consumer to limit the user or disclosure of their sensitive PI.[267] Businesses are not permitted to require a consumer to create an account or provide additional information in order to limit use or disclosure of their sensitive PI.[268]

A covered business must implement **reasonable security procedures and practices** appropriate to the nature of the PI, to protect it from any sort of data breach or unauthorized access, destruction, use, modification, or disclosure.

Finally, businesses must provide **adequate training** to "ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance. . ." are informed about CCPA's requirements and how to direct consumers to exercise their rights.[269]

Enforcement

The CCPA is enforced by the California Privacy Protection Agency and the California Attorney General.[270] Violations of CCPA may result in civil penalties which may result in up to $2,500 per violation or up to $7,500 per intentional violation.[271] However, businesses have 30 days to cure any violation after being notified of noncompliance.

[261] § 1789.130(a)(5)(C).
[262] § 1798.100(b).
[263] *Id.*
[264] *Id.* at (c).
[265] *Id.* at (d).
[266] § 1798.135(a)(1).
[267] § 1798.135(a)(2).
[268] § 1798.135(c)(1).
[269] §§ 1798.130(a)(6), 1798.135(c)(3).
[270] §§ 1798.155 ; 1798.199.90(a).
[271] *Id.*

There is a **limited** civil private right of action for consumers, *only* for data breaches involving PI.[272] A consumer may have grounds to bring a suit if their nonencrypted and nonredacted PI, or email address in combination with a password or security question and an answer that would permit access to the account is subject to an unauthorized access, theft, or disclosure.[273] Further, that breach must have been the result of the business' violation of their duty to implement and maintain reasonable security procedures and practices.[274]

However, consumers must give the business written notice of which CCPA section it violated and allow 30 days to respond in writing that it cured the violations.[275] If the business actually cures the violation, a consumer cannot bring suit.[276]

For More Information:

- Text of the CCPA
- International Association of Privacy Professionals, CCPA-/CPRA-Related Legislation Tracker

[272] § 1798.150(a)(1).
[273] *Id.*
[274] *Id.*
[275] § 1798.150(b).
[276] *Id.*

Virginia's Consumer Data Protection Act (VCDPA)

On March 2, 2021, the Virginia Consumer Data Protection Act was signed into law, making it the second statewide comprehensive privacy law.[277] The VCDPA applies to persons that conduct business in the Commonwealth **or** produce products or services that are targeted to residents of the Commonwealth, **and that:**

i. During a calendar year, control or process personal data of at least 100,000 consumers **or**

ii. Control or process personal data of at least 25,000 consumers **and** derive over 50% of gross revenue from the sale of personal data[278]

However, VCDPA establishes two levels of exemptions: entity level exemptions and data-level exemptions. So, even if an entity meets the above definition, VCDPA exempts any:

1. Body, authority, board, bureau, commission, district, or Virginian agency or any Virginian political subdivision
2. Financial institution or data subject to the Gramm-Leach-Bliley Act
3. Covered entity or business subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act
4. Nonprofit organization
5. Institution of higher education[279]

Next, there are 14 categories of data that are exempted, which largely includes information subject to other laws, such as:

- Health Insurance Portability and Accountability Act (HIPAA)
- Fair Credit Reporting Act (FCRA)
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Driver's Privacy Protection Act
- Farm Credit Act[280]

Covered businesses are also split between "controllers" and "processors" and have varying obligations based on that designation. A controller is the "natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."[281] Whereas the processor is the "natural or legal entity that processes that personal data on behalf of a controller."[282]

Consumers are defined as "a natural person who is a resident of the Commonwealth acting only in an individual or household context."[283] This designation explicitly excludes "natural person[s] acting in a commercial or employment context."[284]

The Act protects Personal Data (PD) which it defines as "any information that is linked or reasonably linkable to an identified or identifiable natural person" but, like CCPA, excludes de-identified data or publicly available information.[285]

---

[277] *See generally* Va. Code. §§ 59.1-575 – 59.1-584 (2023).
[278] § 59.1-576(A).
[279] § 59.1-576(B).
[280] § 59.1-576 (C)(1)-(14).
[281] § 59.1-575.
[282] § 59.1-575.
[283] § 59.1-575.
[284] *Id.*
[285] *Id.* Under the same section, de-identified data "means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person."

However, CDPA casts a wider net in defining "publicly available information" as including not only information that is "lawfully made available through . . . government records" but also:

> Information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.[286]

There is also a separate designation for "sensitive data" which includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data.[287]

Individual Rights

VCDPA explicitly provides for five individual rights. Consumers can invoke their consumer rights at any time by submitting a request to a controller, specifying the consumer rights the consumer wishes to invoke.[288]

1. To confirm whether or not a controller is processing the consumer's PD **and** to access such PD.
2. To correct inaccuracies in the consumer's PD, taking into account the nature of the data and the purposes of the processing of the data.
3. To delete PD provided by or obtained about the consumer.
4. To obtain a copy of the consumer's PD that the consumer previously provided to the controller, in a portable and readily usable format, where the processing is carried out by automated means.
5. To opt out of the processing of PD for the purposes of
    a. Targeted advertising
    b. The sale of personal data
    c. Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Controllers must respond to these requests within 45 days, and, like CCPA, this window may be extended once by 45 additional days, so long as the consumer is informed of the extension within the initial 45-day response period.[289] Controllers must fulfill these requests from consumers for free, up to twice annually per consumer.

However, if a controller is unable to authenticate the request, they will not be required to comply with the request, though they may request that consumers provide additional information to successfully authenticate the identity of the consumer.[290] In the event that a controller declines to take action on a request, they must communicate that to the controller within 45 days.[291] The controller must establish a process for a consumer to appeal the refusal to take action, and if the appeal is denied, the controller must also provide the consumer with a mechanism through which the consumer can contact the Attorney General to submit a complaint.[292]

Obligations on Controllers

[286] *Id.*
[287] § 59.1-575.
[288] § 59.1-577(A).
[289] § 59.1-577(B)(1).
[290] § 59.1-577(B)(4).
[291] § 59.1-577(B)(2).
[292] § 59.1-577(C).

Controllers ae subject to certain obligations under § 59.1-578 related to data transparency.

1. Controllers shall limit the collection of PD to what is adequate, relevant, and reasonably necessary in relation to the purpose for which such data is processed, as disclosed to the consumer.
2. Controllers must not process PD for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such PD is process, as disclosed to the consumer, unless the controller obtains the consumer's consent.
3. Controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the PD they collect. These measures must be appropriate to the volume and nature of the PD at issue.
4. Controllers are prohibited from discriminating against a consumer for exercising any of their rights under the VCPDA, including by denying goods or services, providing a different level of quality of goods, or charging different prices or rates for goods or services.
5. Controllers will not process sensitive data[293] concerning a consumer without obtaining the consumer's consent.

The Privacy Notice

Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

1. The categories of personal data processed by the controller.
2. The purpose for processing personal data.
3. How consumers may exercise their consumer rights and appeal a controller's decision regarding the consumer's request.
4. The categories of personal data that the controller shares with third parties, if any.
5. The categories of third parties, if any, with whom the controller shares personal data.[294]

Additionally, controllers must disclose whether they sell personal data to third parties, or process personal data for targeted advertising, including a manner in which a consumer may opt-out of such processing.[295]

The privacy notice must also include one or more means for consumers to submit a request to exercise their consumer rights. When establishing these mechanisms, controllers must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the controller.[296] Controllers are prohibited from requiring consumers to make an account to exercise these rights.[297]

The Relationship Between Controllers and Processors

Processors must adhere to instructions of controllers and must assist the controller in meeting its obligations under VCDPA. Further, there must be a contract between the controller and processor which governs the processor's data processing procedures.[298] The contract must include:

- Instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.
- Ensure that each person processing personal data is subject to a duty of confidentiality
- Obligate the processor to:
    - delete or return all personal data to the controller as requested at the end of the provision of services

[293] § 59.1-575. (sensitive data includes (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship
[294] § 59.1-578(C)(1)-(5).
[295] § 59.1-578(D).
[296] § 59.1-578(E).
[297] *Id.*
[298] § 59.1-579(B)(1)-(5).

- Make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter
- Allow and cooperate with reasonable assessments by the controller or the controllers' designated assessments.
- Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

Data Processing Assessments

Controllers must conduct and document a data protection assessment of:

1. The processing of PD for purposes of targeted advertising;
2. The sale of PD;
3. The processing of PD for purposes of profiling, where such profiling presents a reasonably foreseeable risk of
    a. unfair or deceptive treatment or unlawful disparate impact on consumers;
    b. financial, physical, or reputational injury to consumers;
    c. a physical or other intrusion upon the solitude or seclusion of consumers or
    d. other substantial injury to consumers.
4. The processing of sensitive data; and
5. Any processing activities involving PD that present a heightened risk of harm to consumers.

Enforcement

Virginia's Attorney General has the sole responsibility of enforcement as there is no private right of action.[299] Prior to initiating an action against a controller or processor, the Attorney General must provide them 30 days' written notice.[300] The controller has 30 days to cure the violation and provide the attorney general with an "express written statement that the alleged violations have been cured and that no further violations shall occur."[301] If the controller fails to cure the violation, the Attorney General may fine them up to $7,500 *for each violation*.[302]

For More Information:

- Text of the Act.
- VPM NPR, Impacts of Virginia's Consumer Data Protection Act

[299] *See* § 59.1-584(A).
[300] § 59.1-584(B).
[301] *Id.*
[302] § 59.1-584(C).

Colorado Privacy Act (CPA)

On July 7, 2021, Colorado became the third state to pass a comprehensive privacy law. The CPA applies to "controllers" that conduct business in Colorado or deliver commercial products or services that are intentionally targeted to Colorado residents and that either

1. Control or process the personal data of 100,000 or more consumers during a calendar year **or**
2. Derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000 or more consumers.[303]

Both the definition of a controller and consumer are quite similar to Virginia's CDPA. Under CPA, a "consumer" is:

- An individual who is a Colorado resident acting only in an individual or household context **and**
- Does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context[304]

The CPA established various individual rights for consumers:

- The right to opt-out
- The right to access
- The right to correction
- The right to deletion
- The right to data portability[305]

To more completely understand these rights, it's important also to know the CPA's standard for "consent." Under CPA, consent means "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data."[306] The CPA additionally includes several examples of what does *not* constitute consent, such as:

- Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;
- Hovering over, muting, pausing, or closing a given piece of content; and
- Agreement obtained through dark patterns.[307]

The CPA requires that controllers provide a reasonably accessible, clear, and meaningful privacy notice that includes:

i. The categories or personal data collected or processed,
ii. The purposes for processing of personal data;
iii. How and where consumers may exercise their rights and how to appeal a controller's action in response to a request;
iv. Categories of personal data shared with third parties; and
v. The categories of third parties with whom the controller shares personal data[308]

[303] Colo. Rev. Stat. 6-1-1304(1)(a),(b)(I),(II).
[304] § 6-1-1303(6)(a),(b).
[305] *See Protect Personal Data Privacy*, Colorado General Assembly, https://leg.colorado.gov/bills/sb21-190
[306] § 6-1-1303(5)
[307] *Id.* (a)-(c).
[308] § 6-1-1308 (1)(a)(I)-(V).

The CPA contains various other obligations on controllers that are similar to those contained in VCDPA and CCPA. Those are:

Transparency	Purpose Specification	Data Minimization	Process Sensitive Data Only with Consumer Consent[309]
Avoid Secondary Use of Personal Data	Duty of Care	Avoid Unlawful Discrimination	

Further, the CPA requires that controllers conduct a data protection assessment when processing personal data that presents a heightened risk of harm to a consumer.[310]

Section 6-1-1311 discusses enforcement of the CPA and establishes that the attorney general and district attorneys have exclusive authority to handle enforcement.[311] Importantly, there is *no private right of action*.[312] Prior to any enforcement action, the attorney general or district attorney must issue a notice of violation to the controller *if a cure is deemed possible*.[313] If the controller fails to cure the violation *within sixty days after receipt* of the notice, the attorney general/district attorney may then bring an action.[314]

For More Information:

- Text of the Act
- Secure Privacy, Comprehensive Guide to the Colorado Privacy Act
- Husch Blackwell, Colorado Privacy Act Resource Center

[309] *Id.* at (2)-(7).
[310] § 6-1-1309(1).
[311] § 6-1-1311(1)(a)
[312] § 6-1-1311(1)(b)
[313] *Id.* at (d).
[314] *Id.*

Illinois Biometric Information Privacy Act ("BIPA")

In 2008, the Illinois legislature passed the Biometric Information Privacy Act ("BIPA") upon findings that "the use of biometric information is growing" and "[m]ajor national corporations have selected the City of Chicago . . . as testing sites for new applications of biometric-facilitated transactions."[315] The Illinois legislature determined that regulations were necessary as "biometric data is unlike other unique identifiers" and considering that "the full ramifications of biometric technology are not fully known."[316]

The Act places limitations upon businesses in the collection, storage, disclosure, and use of biometric information and additionally, provides individuals with a private right of action where businesses fail to comply. BIPA regulates "private entities" which it defines as: "any individual, partnership, corporation, limited liability company association or other group, however organized."[317]

BIPA distinguishes between "biometric identifiers" and biometric information." A "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[318] The Act further contains an extensive list of information that does *not* constitute a biometric identifier, including:

- Writing samples, human biological samples used for valid scientific testing or screening, demographic data, and tattoo or physical descriptions
- Donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act
- Biological materials regulated under the Genetic Information Privacy Act
- information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996
- An X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.[319]

Biometric Information is defined as "any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual."[320]

Obligations on Private Entities

There are several obligations that the BIPA places on private entities. First, a private entity **in possession of** biometric identifiers or biometric information must:

- Create a retention schedule and guidelines for permanently destroying biometric identifiers/information
- Destroy biometric identifiers/information once the initial purpose for collecting or obtaining such identifiers or information has been satisfied OR within 3 years of the individual's last interaction with the private entity, whichever occurs first.
- Must develop a written policy which includes the retention schedule
- Comply with the retention schedule and destruction guidelines, absent a warrant or subpoena.[321]

[315] 740 ILCS 14/5 § 5 (a),(b).
[316] § 5 (c),(f).
[317] *Id.* at § 10 "Private Entity".
[318] *Id.* at "Biometric Identifier".
[319] *Id.*
[320] *Id.* at "Biometric Information" ("does not include information derived from items or procedures excluded under the definition of biometric identifiers")
[321] *Id.* at § 15(a).

Further, private entities cannot collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric information unless it first:

- Informs the subject in writing that a biometric information/identifier is being collected or stored
- Informs the subject in writing of the specific purpose and length of term for which the information is being collected, used, and stored **and**
- Receives a written release[322] executed by the subject of the biometric information/identifier.[323]

Enforcement

Section 20 of BIPA creates a right of action wherein any person aggrieved by a violation of the Act may bring a claim in a State circuit court or may bring a supplemental claim in a federal district court against an offending party.[324]

Where a party brings suit against a private entity that *negligently* violates the Act, the aggrieved party may recover liquidated damages of $1,000 or actual damages, whichever is greater.[325] Where a party brings suit against a private entity that *intentionally or recklessly* violates a provision of the Act, they may recover liquidated damages of $5,000 or actual damages, whichever is greater.[326] Further, a party that prevails may recover reasonable attorneys' fees and additional fees such as expert witness fees and litigation expenses. Additionally, the court may impose additional forms of relief such as an injunction.[327]

In 2019, the Illinois Supreme Court held in *Rosenbach v. Six Flags Entertainment* held that a plaintiff can be considered an "aggrieved person" under the statute and "be entitled to liquidated damages and injunctive relief" without alleging an actual injury. [328]

For More Information:

- Text of the Act
- WilmerHale, Illinois Supreme Court Finds that Biometric Information Privacy Act Claims Accrue with Each and Every Violation
- Bloomberg Law, The Evolution of Biometric Data Privacy Laws

[322] *Id.* at § 10 ("Written release means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment").
[323] *Id.* at § 15(b)(1)-(3).
[324] *Id.* at § 20.
[325] *Id.* at (1).
[326] *Id.* at (2).
[327] *Id.* at (3),(4).
[328] *See Rosenbach v. Six Flags Entm't Corp., 432 Ill. Dec. 654, 129 N.E.3d 1197 (Ill. 2019)* (holding that a plaintiff can be an "aggrieved person" and "be entitled to liquidated damages and injunctive relief" without alleging an actual injury.)

Relevant International Privacy Regulations

General Data Protection Regulations

The General Data Protection Regulation (GDPR) is a general data privacy regulation in the European Union which is generally considered to be the world's strongest set of data protection rules.[329] Central to GDPR is its protection of personal data, which is accomplished through a set of individual rights granted to consumers, and obligations placed on "controllers" or "processors."[330]

The GDPR made a distinction between data processors and data controllers to recognize that not all individuals involved in the processing of data have the same degree of responsibility. However first, GDPR applies to organizations which (1) have an EU established presence (physical locations in the EU) and (2) organizations that process personal data in connection with the "offering of goods or services" or monitoring of individuals' behavior within the EU.[331] Within this group, data controllers may be "a person who determines the purposes for which and the manner in which any personal data are, or are not to be processed."[332] On the other hand, data processors are "any person who processes the data on behalf of the data controller."[333]

Under the GDPR, personal data is information that allows a living person to be directly, or indirectly, identified from data that's available.[334] Further, GDPR created a category of sensitive personal data that are given greater protection, such as information about ethnic or racial origin, political opinions, or religious beliefs.[335]

While GDPR is a complicated regulation, its "key principles" and individual rights may provide an overview of the goals and methods of the regulation as a whole.

GDPR'S KEY PRINCIPLES	GDPR'S INDIVIDUAL RIGHTS
1. Lawfulness 2. Fairness and transparency 3. Purpose limitation 4. Data minimization 5. Accuracy 6. Storage limitation 7. Integrity and confidentiality 8. Accountability	1. Right to Transparent Information 2. Right to be Informed 3. Right of Access 4. Right to Rectification 5. Right to Erasure 6. Right to Restriction of Processing 7. Right to Data Portability 8. Right to Object 9. Additional rights re: automated decision making & profiling

[329] Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK* (Mar. 24, 2020) https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
[330] (EU) 2016/679 (EU GDPR) Ch. 1, Art. 3.
[331] *Id.*
[332] (EU) 2016/679 (EU GDPR) Ch. 1, Art.3(7).
[333] (EU) 2016/679 (EU GDPR) Ch. 1, Art.3(8).
[334] (EU) 2016/679 (EU GDPR) Ch. 1, Art.3(1).
[335] (EU) 2016/679 (EU GDPR) Ch. 1, Art.9(1).

For More Information:

- Text of the Regulation
- Guide to GDPR Compliance
- Enforcement Tracker, GDPR Enforcement Tracker – List of GDPR Fines

Data Brokers

One enormous player in the privacy ecosystem that is able to fly under the radar are data brokers. The first difficulty in exploring this concept arises when trying to define data brokers. In a 2016 report, Upturn and the Open Society Foundation found that "[t]here is no authoritative definition of 'data broker' on either side of the Atlantic."[336] Still, the report proposed a working definition:

> A company or business unit that earns its primary revenue by supplying data *or inferences* about people gathered mainly from sources other than the data subjects themselves.[337]

There are several markets that rely on or use brokered data. Those include:

Health. Data brokers are able to pull "longitudinal information"[338] from hospitals, doctors records, prescriptions, insurance claims, and laboratory tests.[339] One company, IMS Health, receives some portion of the electronic medical records from three quarters of all U.S. retail pharmacies.[340] Organizations that sell this information strip records of Social Security numbers, names and detailed addresses to protect people's privacy.[341] However, big data presents issues of re-identification, undermining anonymization of data.

Identity Verification. An FTC report outlines three identity verification products sold by data brokers.[342] Data brokers offer a scoring format which corresponds to the level of risk of a given transaction. The report explains the function of the scoring format in simple terms:

> For a consumer with a high risk score, the explanatory codes could state that the SSN provided by the consumer is associated with a deceased individual, the address used by the consumer has been associated with fraud or is a prison address, the SSN has been used very frequently in a short period of time, or the SSN has been attributed to an address other than the one submitted by the consumer.[343]

Next, data brokers may offer a quizzing format which seeks verification of identity from the consumer by asking questions such as "Which of these is a zip code where you have lived?" or "what is your mother's maiden name?" This product may also be used in conjunction with the scoring format to determine how many questions a customer must answer correctly depending on their risk score.[344] Finally, there is the "match/no match" format, wherein information provided by the consumer must match the information that the data broker has on file. [345]

---

[336] Aaron Rieke, Harlan Yu, David Robinson, Joris von Hoboken, *Data Brokers in an Open Society*, Open Society Foundation (2016).
[337] *Id* at 3 (emphasis added).
[338] *What are Longitudnal Data?*, National Center for Analysis of Longitudnal Data in Education Research, ("a dataset is longitudinal if it tracks the same type of information on the same subjects at multiple points in time").
[339] Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Scientific American (Feb. 1, 2016) https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/
[340] *Id.*
[341] *See* Justin Sherman, *Big Data May Not Know Your Name. But it Knows Everything Else*, Wired (Dec. 19, 2021) https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/.
[342] *See* Federal Trade Commission, *Data Brokers, A Call for Transparency and Accountability* (May 2014) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[343] *Id.*
[344] *Id.*
[345] *Id.*

Fraud Detection. For fraud detection, a consumer's purchase history may be used to detect fraudulent purchase patterns.[346] Many individuals have likely had a bank place a hold on their account due to a detection of unusual purchases and will be familiar with this model.[347] Companies may also cross check delivery addresses with information collected from data brokers to ensure the address is actually associated with the listed customer.[348]

Advertising and Marketing. Consumer information is often used to create targeted ads. Simply stated, the information and inferences provided by data brokers enables companies to "more accurately target consumers for an advertising campaign, refine product and campaign messages, and gain insights and information about consumer attitudes and preferences."[349]

Government and Law Enforcement. Government and Law Enforcement are also notable consumers and buyers of brokered data, spending millions on both public and nonpublic data.[350] The Electronic Communications Privacy Act functionally contains a loophole wherein Law Enforcement is able to obtain data from data brokers directly and circumvent requirements that they must use legal process to obtain data directly from service providers.[351]

Credit and Insurance. Nearly all major financial institutions rely on data brokers to supply data which helps lenders and insurers "set prices for financial products, manage their risk, and comply with regulations."[352]

Education. There is a substantial market for *student* data specifically, both for ventures which claim to have a nexus with education, and with those for marketing purposes.[353]

People Search Sites. This is an enormous industry, worth an estimated $200 billion, which as of now is largely unregulated.[354] As discussed in *Transparency and the Marketplace for Student Data*, students represent an important consumer base – they cite one data broker which advertises high school students as a "brand conscious and tech savvy group of consumers," going so far as to recommend that their data be used for products such as "formal wear and limo services," or "smart phones and personal electronics."[355]

Implications

There are a variety of concerns with the data broker industry including the widespread discriminatory effects resulting from data brokers use of algorithms and the advent of surveillance capitalism.[356] Beyond these harms, law

[346] *Id.*
[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] Carey Shenkman, Sharon Bradford Franklin, et al., *Legal Loopholes and Data For Dollars*, Center for Democracy and Technology (Dec. 2021) https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.
[351] *Id.*
[352] Aaron Rieke, Harlan Yu, et al., *Data Brokers In An Open Society*, Open Society Foundations (Nov. 2016) www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf
[353] N. Cameron Russell, Joel R. Reidenberg et al., *Transparency and the Marketplace for Student Data*, 22 Va. J.L. & Tech. 107 (Spring 2019).
[354] David Lazarus, *Column: Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, LA Times (Nov. 5, 2019) https://www.latimes.com/business/story/2019-11-05/column-data-brokers; N/A, *Data Brokers*, Electronic Information Privacy Center, https://epic.org/issues/consumer-privacy/data-brokers/
[355] *Id.*
[356] Justin Sherman, *Data Brokers Are a Threat to Democracy*, Wired (Apr. 13, 2021) https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/; *Data Brokers supra* 99; *see also* John Laidler, *High Tech is Watching You*, The Harvard Gazette (Mar. 4, 2019) https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ (Defining surveillance capitalism "as the unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products. . .")

enforcement consistently purchase data from data brokers, allowing them to skirt warrant requirements if they were to obtain the data traditionally.[357]

The ability for law enforcement and government agencies to circumvent warrant requirements and buy data to use in criminal investigations has significant implications for the realization of fourth amendment protections. This tension is most clearly demonstrated by the buying and selling of location data. In 2018, the Supreme Court ruled in *Carpenter v. United States* that under the Fourth Amendment, police must obtain a warrant prior to obtaining historical cell site location information derived from cell carriers.[358] However, the holding did not explicitly speak to the legality of data brokers providing this same information to law enforcement.

Companies like Fog Data Science readily exploit this gap in Fourth Amendment protections. Fog Data Science is a company that purchases raw geolocation data originally collected from cell phones and other smart devices.[359] According to the company, Fog purchases "billions of data points" around the United States originally sources from "tens of thousands" of mobile apps.[360] This data is entered into a searchable database which law enforcement may access for a yearly subscription fee.[361] Consequently, police with access to the database, sometimes without a warrant, "have the ability to track the precise movements of hundreds of millions of Americans as they go about their day."[362]

After the Supreme Court's holding in *Dobbs v. Whole Women's Health*, which overturned *Roe v. Wade*, reproductive justice and privacy advocates have been alerting how today's "unprecedented digital surveillance" increases the potential of harm to abortion seekers.[363] Since location data is already being used for other investigations, its' use in criminal abortion investigations wouldn't be a big leap.[364] Advocates are specifically concerned about the use of Geofencing, whether through databases like Fog Data Science's, or through geofence warrants.[365] Law enforcement determining which devices were present at an abortion clinic are often just the beginning of an investigation – for instance, if police obtain location data via warrant from Google, they may often follow up to request more details such as email content, names, and associated phone numbers.[366] While Google has responded to concerns by pledging to delete abortion clinic visits from the location history of its users, only time will tell what role this tech giant will play in the fight for reproductive justice.[367]

---

[357] Sherman *supra* 103.
[358] Bennett Cyphers & Aaron Mackey, *Fog Data Science Puts our Fourth Amendment Rights up for Sale*, Electronic Frontier Foundation (Aug. 31, 2022) https://www.eff.org/deeplinks/2022/08/fog-data-science-puts-our-fourth-amendment-rights-sale
[359] Matthew Guariglia, *What is Fog Data Science? Why is the Surveillance Company so Dangerous?*, Electronic Frontier Foundation (Aug. 31, 2022) https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous.
[360] *Id.*
[361] *Id.*
[362] *Id.*
[363] Adam Schwarz, *Congress Probes How Location Data Brokers Threaten Reproductive Privacy*, Electronic Frontier Foundation (Jul. 12, 2022) https://www.eff.org/deeplinks/2022/07/congress-probes-how-location-data-brokers-threaten-reproductive-privacy
[364] *See* Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, Politco (Jul. 18, 2022) https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906
[365] *Id.*; *see also* Amber Kemmis, *What is GeoFencing? Everything You Need to Know About Location-Based Marketing*, SmartBug (Jan. 8, 2020) https://www.smartbugmedia.com/blog/what-is-geofencing ("Geofencing is a location-based service in which an app or other software program uses radio frequency identification (RFID), Wi-Fi, GPS, or cellular data to trigger a targeted marketing action (such as a text, email, social media advertisement, app notification) when a mobile device or RFID tag enters or exits a virtual geographic boundary, known as a geofence.")
[366] *Id.*
[367] *See* Nico Grant, *Google Says It Will Delete Location Data When Users Visit Abortion Clinics*, New York Times (Jul. 1, 2022) https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html