

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Data Privacy Individual Action Plan** (Revised 2021)

**United States (submitted 2021)**

1. **Introduction**

The United States has multiple federal statutes that protect personal information and data, and these laws primarily regulate certain sectors or categories of data, for example health, financial, and children’s data. The U.S. Federal Trade Commission also protects consumers’ personal data under its statutory authority to enforce against unfair and deceptive acts in or affecting commerce. This report focuses on federal privacy law, but it should be noted that several U.S. States have passed laws relating to consumer protection and data privacy. For example, California, Colorado, and Virginia have recently enacted comprehensive data protection laws aimed at protecting consumers. In addition, every state has enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. and every state has a consumer protection law that prohibits deceptive practices, and many prohibit unfair or unconscionable practices as well.

1. **United States Federal Privacy Laws (2021)**

|  | APEC Principle / Commentary / Implementation guidance | **Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [[1]](#footnote-2)** | **Provision[[2]](#footnote-3)** | **Sanction[[3]](#footnote-4)** | **Results/ Status[[4]](#footnote-5)** |
| --- | --- | --- | --- | --- | --- |
| A | Is privacy a constitutionally protected right in your economy? | The United States Constitution protects against government infringement of certain privacy rights of individuals. | U.S. Constitution, Amendments 4, 14. |  |  |
| B | If not, what other available legislation deals with privacy or confidentiality of personal information. | In the United States, there are federal and state statutes and regulations that deal with personal information privacy and data security, both generally and on an industry-sectoral basis. In addition, there are self-regulatory frameworks that reflect the APEC privacy principles.  The primary federal statutes, regulations, and an example of a self-regulatory framework governing the private sector’s collection, use handling and disclosure of personal consumer information are identified below. |  |  |  |
| 1 | ***I Preventing Harm***  **(Ref. Para. 20)**  Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information. | ***The* *Fair Credit Reporting Act (FCRA),*** 15 U.S.C. § 1681 et seq. | The FCRAprotects consumer information collected by consumer report­ing agencies such as credit bureaus, medical information companies and tenant screening services. By limiting the use of such “consumer report” information to certain “permissible purposes,” by requiring furnishers of customer information to consumer reporting agencies to take steps to ensure the accuracy of that information, by limiting the scope of such information, by requiring consumer reporting agencies to establish reasonable procedures to assure maximum possible accuracy of the in­formation they report on consumers, and by requiring any person who maintains or otherwise possesses consumer report in­formation to properly dispose of the information after they have used it, the FCRA seeks to prevent harmful use of consum­er report information. 15 U.S.C. §§ 1681, 1681b(a), 1681c(a), 1681c-1, 1681c-2, 1681e(b), 1681s-2(a), 16 C.F.R. Part 660, 12 C.F.R. Part 1022, Subpart E, 1681w, 16 C.F.R. Part 682.  In addition, the FCRA provides specific protections to limit harm to consumers victimized by identity theft. For example, such consumers are permitted to require nationwide credit bureaus to insert a “fraud alert” in their files, and to block reporting of information that results from identity theft. 15 U.S.C. §§ 1681c-1, 1681c-2. Moreover, creditors and financial institutions must implement policies and procedures to identify and mitigate against identity theft. 15 U.S.C. § 1681m(e). 16 C.F.R. Part 681. | The FCRA provides for civil liability for willful and negligent noncompliance. The remedies for willful noncompliance are more stringent. 15 U.S.C. §§ 1681n, 1681o. The FCRA also provides for criminal sanctions for obtaining consumer report information under false pretenses. 15 U.S.C. § 1681q. The Act is enforced by the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) and state authorities, as well as private litigants. It allows courts to impose penalties of up to $4,111 per knowing violation in actions brought by the FTC. 15 U.S.C. § 1681s(a); 16 C.F.R. § 1.98(m). | Signed into law on October 26, 1970. |
| ***The* *Gramm-Leach-Bliley Act (GLBA)*,** Subchapter I (Disclosure of Nonpublic Personal Information) 15 U.S.C. § 6801 et seq. and Subchapter II, (Fraudulent Access to Financial Information) 15 U.S.C. § 6821 et seq., and implementing regulations at 16 C.F.R. Parts 313 and 314 (FTC). We only include the citations to the FTC rule by way of an example. Citations to the comparable and consistent rules of each of the banking agencies and other regulators that enforce GLBA are not included. In addition to these rules, the four banking agencies issued additional interagency guidance interpreting the information security rules to require banks to notify customers of information security breaches involving their personal information. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (March 29, 2005). | The GLBA requires the FTC, along with the Federal functional regulators and State Insurance Commissioners to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information. Due to the sensitive nature of consumers’ financial information and the potential for significant harm resulting from misuse of such information, the GLBA and its implementing regulations protecting consumers’ financial information reflect the “Preventing Harm” principle. 15 U.S.C. § 6801.  Additionally, Title X of the Dodd-Frank Act Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) granted rulemaking authority for most provisions of Regulation P, Subtitle A of Title V of GLBA – which addresses the right of financial institutions to share customer financial information and the corresponding right of consumers to protect the confidentiality of that information - to the Consumer Financial Protection Bureau (CFPB).[[5]](#footnote-6) The Dodd-Frank Act also granted authority to the CFPB to examine and enforce compliance with these statutory provisions and their implementing regulations with respect to entities under CFPB jurisdiction. | The GLBA is enforced by the respective governmental authorities responsible for oversight of the financial institutions, with residual jurisdiction to the FTC. In enforcing their respective rules, the agencies may obtain a range of civil remedies, including, in the case of the FTC, the full range of relief available under the FTC Act. 15 U.S.C. § 41 et seq.; 15 U.S.C. §§ 6805, 6822, which states that “Except as provided in subsection (b), compliance with this subchapter shall be enforced by the Federal Trade Commission in the same manner and with the same power and authority as the Commission has under the Fair Debt Collection Practices Act to enforce compliance with such Act.” In addition, obtaining customer information by false pretenses may carry criminal penalties. 15 U.S.C. § 6821(b), 6823. The federal banking agencies may use any remedy available under Section 8 of the Federal Deposit Insurance Act, 12 U.S.C. § 1818, including cease and desist orders, restitution, and civil money penalties. | Signed into law on November 12, 1999. |
| ***The Children’s Online Privacy***  ***Protection Act (COPPA)***, 15 U.S.C. § 6501 et seq., and implementing regulation at 16 C.F.R. Part 312. | COPPA applies to operators of websites directed to children under 13 years old or operators that have actual knowledge that they have collected personal information from such children. This Act protects children’s privacy by giving parents the tools to control what information operators can collect from children online and how they can use and disclose the information. By protecting the privacy of children, the Act reflects the “Preventing Harm” principle. | COPPA deems violations to be unfair or deceptive business practices and its mandates are enforceable by the Federal Trade Commission, other federal regulators against entities within their specific jurisdictions, and State authorities. Violations carry civil monetary penalties. COPPA includes self-regulatory compliance and monitoring options. | Signed into law October 21, 1998. |
| ***The Federal Trade Commission Act (FTC ACT)***, 15 U.S.C. § 41 et. seq. | Section 5 of the FTC Act conveys broad authority to the FTC to combat “unfair or deceptive” business practices. The FTC uses this broad authority to protect consumer privacy interests where deceptive or unfair business practices result in harmful privacy violations. 15 U.S.C. § 45.  Section 5 also grants the FTC the authority to as a backstop enforcer for the United States with regard to companies’ representations of their APEC Cross-Border Privacy Rules (CBPR) System certification, as well as their underlying business practices pursuant to the CBPR System program requirements. | For violations of Section 5 of the FTC Act, the FTC may obtain injunctive relief under 15 U.S.C. § 53(b) or proceed with an administrative complaint which may lead to the issuance of a cease and desist order. For violations of rules respecting unfair or deceptive practices or violations of cease and desist orders issued pursuant to Section 5, the FTC may obtain rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification respecting the rule violation or the unfair or deceptive act or practice pursuant to 15 U.S.C. § 57b. The federal banking agencies also may enforce section 5 with respect to the entities they regulate under section 8 of the Federal Deposit Insurance Act. 12 U.S.C. § 1818. | Signed into law on September 26, 1914. |
| ***The Drivers Privacy Protection Act of 1994 (DPPA)***, 18 U.S.C. § 2721 et seq. | The DPPA protects individuals’ personal information collected by state departments of motor vehicles. By limiting the disclosure of such personal information to certain “permissible uses”, and by requiring consent of the individual for any re-sale and redisclosure of such information by authorized users, including businesses, for purposes other than the “permissible uses”, the Act reflects the “Preventing Harm” principle. 18 U.S.C. § 2721. | DPPA provides for criminal fines and civil penalties. It is enforced by federal authorities as well as private litigants. 18 U.S.C. §§ 2723, 2724. | Signed into law on September 13, 1994. |
| ***Health Insurance Portability and Accountability Act (HIPAA),*** Pub. L. 104-191 §§ 262 & 264) | HIPAA applies to “covered entities” that are providers of care, payers of claims, or clearinghouses that support those functions who engage in electronic claims transactions. HIPAA is implemented by several rules, including a Privacy Rule that permits disclosure of individually identifiable information for treatment, payment, and health care operations, but otherwise prohibits disclosures except as authorized by the Rule. Such disclosures must be limited to the minimum necessary to achieve the purposes of the disclosure. The Privacy Rule also requires security safeguards that reflect the “Preventing Harm” principle. |  | Signed into law on August 21, 1996. |
| ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | The Communications Act, as enforced by the Federal Communications Commission (FCC), protects the privacy of consumer information collected by telecommunications carriers. It imposes a duty on every telecommunications carrier to protect the confidentiality of customers’ personal information, 47 U.S.C. § 222(a), and limits the power of such carriers to use or disclose that information, 47 U.S.C. §§ 222(b)-(d), 551. | Under the Communications Act, a person whose privacy rights were violated by a telecommunications carrier may file a complaint with the FCC, 47 U.S.C. § 208, or seek damages in federal court, 47 U.S.C. §§ 206, 551(f), but may not pursue both remedies, 47 U.S.C. § 207. The FCC has the power both to issue injunctions against telecommunication carriers for violations of the Communications Act, and to fine them for failure to obey such orders. 47 U.S.C. § 205. Moreover, any person who willfully and knowingly violates a provision of the Communications Act may be both fined and sentenced to imprisonment, 47 U.S.C. § 501. Finally, any person who willfully and knowingly violates a regulation made pursuant to the Communications Act may be fined. 47 U.S.C. § 502. | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Restore Online Shoppers’ Confidence Act of 2010,* 15 U.S.C. §§ 8401 - 8405.** | The Restore Online Shoppers’ Confidence Act protects consumers from having their credit cards or other financial accounts charged by a post-transaction third party seller without the informed consent of the consumer and disclosure to the consumer of all material terms. 15 U.S.C. § 8402. The Act also protects consumers from charges through a negative options feature unless the consumer is provided with a clear and conspicuous disclosure and the consumer’s informed consent is obtained. 15 U.S.C. § 8403. | Under the Restore Online Shoppers Confidence Act, the FTC can seek penalties under the FTC Act for violations. 15 U.S.C. § 8404. The Act also authorizes the Attorneys General of states to bring a claim on behalf of their citizens in federal court for injunctive relief. 15 U.S.C. § 8405. | Signed into law on December 29, 2010. |
| 2 | ***II Notice***  **(Ref. Para. 21-23)**  Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should  include:  a) the fact that personal information is being collected;  b) the purposes for which personal information is collected;  c) the types of persons or organizations to whom personal information might be disclosed;  d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;  e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.  All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.  It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. | ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | Consumer reporting agencies obtain their information from creditors and other third parties and are not generally required to notify consumers beforehand. However, the FCRA provides for extensive consumer disclosures upon request by consumers. 15 U.S.C. § 1681g.  Businesses that use consumer reports for employment purposes must notify the consumer and obtain authorization in advance. 15 U.S.C. § 1681b(b)(2). Financial institutions must provide a written notice advising con­sum­ers if they plan to report negative information to credit bureaus. 15 U.S.C. § 1681s-2(a)(7). Risk-based pricing notices are required to consumers who receive credit on materially less favorable terms than a creditor’s other customers. 15 U.S.C. § 1681m(h). ), 16 C.F.R. Part 640, 12 C.F.R. Part 1022, Subpart H.  All consumer report users must, when they take adverse action based on a consumer report, provide the consumer with a notice that identifies the consumer reporting agency that provided the report, informs the consumer of the consumer’s right to a free copy of their report from the consumer report agency if the consumer requests it within 60 days, informs the consumer of the consumer’s right to dispute the accuracy or completeness of any information provided by the consumer reporting agency, and provides the consumer’s credit score, if a score was used in taking the adverse action. 15 U.S.C. §1681m(a).  Before a company shares certain consumer information with an affiliate, it must notify the consumer about the sharing and give the consumer an opportunity to opt out. 15 U.S.C. § 1681a(d)(2)(A)(iii). |  | Signed into law on October 26, 1970. |
|  | ***The Gramm-Leach-Bliley Act (GLBA),***Subchapter I (Disclosure of Nonpublic Personal Information) 15 U.S.C. § 6801 et seq. | The GLBA requires that financial institutions provide consumers with notice of their privacy policies and the opportunity, generally, to opt out of the sharing of their information with third parties for marketing purposes or any form of sharing not covered by one of the exceptions in the GLBA. 15 U.S.C. § 6802, 6803; 16 C.F.R. §§ 313.4-313.10, 313.13.  Additionally, under the GLBA, financial institutions must disclose in their privacy notices each category of information collected from and about consumers. 15 U.S.C. § 6803(a)(1). Financial institutions must follow their stated practices and may only disclose the information they collect as stated in the notice or as permitted by specified exceptions in the rule. 16 C.F.R. §§ 313.13- 313.15 and §§ 313.4-313.6.  Furthermore, companies that receive consumers' personal information from a financial institution may only reuse or redisclose such information in limited circumstances. 15 U.S.C. § 6802(c); 16 C.F.R. § 313.11. |  | Signed into law on November 12, 1999. |
| ***The Children’s Online Privacy Protection Act (COPPA),***15 U.S.C. § 6501 et seq; 16 C.F.R. Part 312. | The COPPA requires operators to post notice of their information practices on their website and directly send such notice to parents when seeking parental consent to collect children’s personal information. 15 U.S.C. § 6502(b)(1); 16 C.F.R. § 312.4. |  | Signed into law on October 21, 1998. |
| ***Health Insurance Portability and Accountability Act (HIPAA),***Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164 | The HIPAA Privacy Rule requires that covered entities provide individuals with adequate notice in plain language of the uses and disclosures of protected health information that the covered entity may make, the individual’s rights, and the covered entity’s legal duties with respect to protected health information. 45 C.F.R. § 164.520. |  | Signed into law on August 21, 1996. |
| ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | The Communications Act requires that a telecommunication carrier provide notice to its customers of their personal information privacy rights prior to soliciting them for approval in using that information to market services to them unlike those they already have. 47 C.F.R. § 64.2007(a), (f).  Moreover, the Act requires that cable operators in particular clearly and conspicuously provide notice of various privacy rights to their customers in writing at the time service begins, and annually thereafter. Thus, cable operators must provide notice of what personal information may be collected - and for what purpose - and explain how that information may be disclosed to others. Customers are also to be given notice of both the statutory limitations governing the use of that information by the cable operator, and the statutory means by which they can enforce those limits. The Act also requires that cable customers be provided with notice of how to access the information collected. 47 U.S.C. § 551(a)(1).  These notice requirements also apply to open video systems. 47 C.F.R. § 76.1510. |  | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),***15 U.S.C. §§ 7701-7713, applicable to commercial electronic e-mail messages. | CAN-SPAM requires unsolicited commercial e-mail messages to be identified as solicitation and to include opt-out instructions and the sender's physical address. It prohibits the use of deceptive subject lines and false headers in such messages. 15 U.S.C. § 7704. | Under CAN-SPAM, many federal agencies, including the FTC and the Department of Justice, certain law enforcement authorities, and Internet service providers, may file civil suits to halt unlawful spammers. 15 U.S.C. § 7703, 7706. | Signed into law on December 16, 2003. |
| 3 | ***III Collection Limitation***  **(Ref. Para. 24)**  The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. | ***The Gramm-Leach-Bliley Act (GLBA),***Subchapter I (Disclosure of Nonpublic Personal Information) 15 U.S.C. § 6801 et seq. | Under the GLBA, financial institutions must disclose in their privacy notices each category of information collected from and about consumers. 15 U.S.C. § 6803(a)(1).  Financial institutions must follow their stated practices and may only disclose the information they collect as stated in the notice or as permitted by specified exceptions in the rule.[[6]](#footnote-7) 16 C.F.R. §§ 313.13- 313.15 and §§ 313.4-313.6.  In addition, companies that receive consumers' personal information from a financial institution may only reuse or redisclose such information in limited circumstances. 15 U.S.C. § 6802(c); 16 C.F.R. § 313.11. |  | Signed into law on November 12, 1999. |
| ***The Children’s Online Privacy Protection Act (COPPA),*** 15 U.S.C. § 6501 et seq; 16 C.F.R. Part 312 | COPPA provides for use limitations in that it requires operators to send notice of and obtain parental consent for the types of information collected and how it will be used or shared with third parties. 15 U.S.C. § 6502(b)(1); 16 C.F.R. §§ 312.3, 312.4, 312.5.  COPPA also prohibits conditioning a child’s participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity. Lastly, COPPA requires parental consent for the collection, use and disclosure of personal information from children. 15 U.S.C. §§ 6501, 6502(b)(1); 16 C.F.R. §§ 312.3, 312.7. |  | Signed into law October 21, 1998. |
| ***Health Insurance Portability and Accountability Act (HIPAA),***Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164 | HIPAA does not generally limit what information a covered entity may collect from an individual. However, it does require that when requesting protected health information from another covered entity, it must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The “minimum necessary” standard also applies to using or disclosing, protected health information. 45 C.F.R. § 164.502. |  | Signed into law on August 21, 1996. |
| ***Electronic Communications Privacy Act (ECPA),***18 U.S.C. § 2510 et seq. | ECPA prohibits, with certain exceptions, interception of electronic communications without the consent of at least one party to the communication. 18 U.S.C. § 2511. | ECPA imposes civil liability. Court may award damages, attorneys’ fees and costs. 18 U.S.C. § 2520. Certain violations may carry criminal liability. | Signed into law on October 21, 1996. |
| ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA limits the use of consumer report information to certain “permissible purposes” unless the consumer consents to different uses. 15 U.S.C. § 1681b(a). Users of consumer reports must certify that they will use the information only for that purpose. 15 U.S.C. § 1681e(a). The FCRA generally prohibits creditors from obtaining or using medical information pertaining to a consumer in connection with any determination of the consumer’s eligibility or continued eligibility for credit, subject to certain exceptions. 15 U.S.C. 1681b(g); 12 C.F.R. Part 1022, Subpart D. |  | Signed into law on October 26, 1970. |
| ***The Federal Trade Commission Act (FTC ACT),***15 U.S.C. § 41 et. seq. | Under Section 5 of the FTC Act, the FTC may hold companies to any use limitations established by their privacy notices. Failing to abide by the representations made in a privacy notice is a “deceptive” business practice. Also, it is an “unfair” practice to make a material change to a privacy policy and then retroactively apply the new policy to information collected under the earlier policy without consumers’ consent. 15 U.S.C. § 45. |  | Signed into law on September 26, 1914. |
| 4 | ***IV Use of Personal Information***  **(Ref. Para. 25)**  Personal information collected should be used only to fulfill the purposes of  collection and other compatible or related purposes except:  a) with the consent of the individual whose personal information is collected;  b) when necessary to provide a service or product requested by the individual; or,  c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. | ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA limits the use of consumer report information to certain “permissible purposes” unless the consumer consents to different uses. 15 U.S.C. § 1681b(a). Users of consumer reports must certify that they will use the information only for that purpose. 15 U.S.C. § 1681e(a).  The FCRA generally prohibits creditors from obtaining or using medical information pertaining to a consumer in connection with any determination of the consumer’s eligibility or continued eligibility for credit, subject to certain exceptions. 15 U.S.C. 1681b(g); 12 C.F.R. Part 1022, Subpart D. |  | Signed into law on October 26, 1970. |
| ***Restore Online Shoppers’ Confidence Act,* 15 U.S.C. §§ 8401 - 8405.** | The Restore Online Shoppers’ Confidence Act prohibits an initial merchant from disclosing a credit card, debit card, bank account, or other financial account number, or other billing information that is used to charge a customer of the initial merchant, to any post-transaction third party seller. (This practice is sometimes referred to as data-pass, and the act prohibits the use of data-pass to facilitate the deceptive internet sales transaction described above). 15 U.S.C. § 8401, 8402(b). |  | Signed into law on December 29, 2010. |
| ***The Drivers Privacy Protection Act of 1994* (DPPA)**, 18 U.S.C. § 2721 et seq. | The DPPA limits the use of individuals’ personal information to certain “permissible uses” outlined in Section B of 18 U.S.C. § 2721 unless the individual consents to different uses. 18 U.S.C. § 2721 |  | Signed into law on September 13, 1994. |
| ***Health Insurance Portability and Accountability Act (HIPAA)***, Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164. | The HIPAA Privacy Rule is mostly a use limitation rule. While uses and disclosures of protected health information are permitted without consent for treatment, payment, or health care operations, other uses are divided into three categories: those for which authorization is required (opt in), those for which an opportunity to agree or object is required (opt out), and those for which an authorization or opportunity to object is not required. For those disclosures requiring authorization, the form and content of authorizations is specified. 45 C.F.R. § 164.506-14. |  | Signed into law on August 21, 1996. |
| ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | Under the Communications Act, a telecommunications carrier may only use or disclose the personal information of customers in order to effectively provide the services requested by the customer. 47 U.S.C. §§ 222(c)(1), 222(d)(1)-(3), 551(b)-(c).  This permissible use includes the telecommunication carrier’s right to use such information to offer additional services to the customer which are similar to those services he already has. For example, if the customer already has basic cable, the telecommunications carrier can use personal information about the customer to market premium cable services to him. 47 C.F.R. § 64.2005(a). As well, personal customer information may be used or disclosed as required by the government, 47 U.S.C. §§ 222(c)(2)(D), 222(d)(4), 551(h), and in any way expressly consented to by the customer, 47 U.S.C. §§ 222(c)(2), 551(b)-(c); 47 C.F.R. § 64.2005(b). Finally, in regard to cable operators specifically, the Act requires that all personal information must be destroyed when it is no longer necessary. 47 U.S.C. § 551(e). This requirement also applies to open video systems. 47 C.F.R. § 76.1510. |  | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),***15 U.S.C. §§ 7701-7713, applicable to commercial electronic e-mail messages. | CAN-SPAM requires unsolicited commercial e-mail messages to be identified as solicitation and to include opt-out instructions and the sender's physical address. Senders must honor requests to opt-out within 10 business days. 15 U.S.C. §7704. |  | Signed into law on December 16, 2003. |
| ***Electronic Communications Privacy Act (ECPA),***18 U.S.C. § 2510 et seq. | ECPA prohibits any person, with certain exceptions, from disclosing electronic communications without the consent of at least one party to the communication. 18 U.S.C. § 2511 |  | Signed into law on October 21, 1996. |
| ***Family Educational and Privacy Rights Act (FERPA),***20 U.S.C. § 1232g, applicable to all schools that receive funds under an applicable program of the U.S. Department of Education. | With certain limited exceptions, schools cannot disclose a student’s information without the student’s consent (or the parent’s consent if the student is a minor). 20 U.S.C. § 1232g(b). | Entities that violate FERPA are not eligible for funding from the applicable program. 20 U.S.C. § 1232g(b). | Signed into law on August 21, 1974. |
| ***Video Privacy Protection Act (VPPA),***18 U.S.C. § 2710, applicable to businesses that rent, sell or deliver pre-recorded videos. | The VPPA restricts businesses from disclosing personally identifiable video rental or purchase records without the consumer’s written consent. 18 U.S.C. § 2710(b). |  | Signed into law on November 5, 1998. |
| ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA allows the use of consumer report information for employ­ment purposes only with the written authorization of the consumer. 15 U.S.C. § 1681b(b)(2). In addition, it provides for the disclosure and use of consumer report information other than for a “permissible purpose” only under limited circumstances. 15 U.S.C. § 1681b(a)-(c). The FCRA also allows consumers to place a security freeze that prohibits a consumer reporting agency from disclosing the contents of the consumer’s consumer report, except pursuant to certain exceptions. 15 U.S.C. § 1681c-1(i).  The FCRA allows consumers to “opt out” of credit bureau prescreening for credit or insurance solicitations, and of certain communications of information among affiliated parties. 15 U.S.C. §§ 1681a(d)(2)(A)(iii), and 1681b(e). The FCRA allows consumers to “opt out” of being sent solicitations based on the sharing of certain information among affiliates. 15 U.S.C. § 1681s-3.  Additionally, although the FCRA does not limit collection, it limits what information may be included in a consumer report and fur­nished to users of such reports. For example, certain dated information may not be included in certain consumer reports. 15 U.S.C. § 1681c(a). Also, the FCRA requires businesses that obtain consumer reports or any consumer information derived from consumer reports to properly dispose of the information to prevent its subsequent use for improper purposes. 15 U.S.C. § 1681w, 16 C.F.R.§ 682.3. |  | Signed into law on October 26, 1970. |
| ***The Gramm-Leach-Bliley Act (GLBA),***Subchapter I (Disclosure of Nonpublic Personal Information) 15 U.S.C. § 6801 et seq. | The GLBA, generally, allows consumers to opt out of the sharing of their information with third parties, unless it (1) discloses to the consumer that such information may be disclosed; (2) gives the consumer an opportunity to opt out; and (3) explains to the consumer how to opt out. 15 U.S.C. § 6802(b); 16 C.F.R. §§ 313.7, 313.10, cf. 313.13 This includes a joint-marketing exception if that agreement complies with 15 U.S.C 6804 implementing regulations, that the consumer was given notice, and the third party agrees to maintain the confidentiality of the information. |  | Signed into law on November 12, 1999. |
| ***The Children’s Online Privacy Protection Act (COPPA),***15 U.S.C. § 6501 et seq; 16 C.F.R. Part 312. | COPPA allows parents to withhold or withdraw consent for the collection, use or maintenance of information about their child and a parent may give consent to the collection and use but withhold consent to the disclosure of information to third parties. 15 U.S.C. § 6502(b)(1); 16 C.F.R. §§ 312.3 and 312.5. |  | Signed into law on October 21, 1998. |
| ***The Drivers Privacy Protection Act of 1994 (DPPA),***18 U.S.C. § 2721 et seq. | The DPPA provides for the disclosure and use of individuals’ personal information other than for a “permissible use” if the individual gives his or her consent. 18 U.S.C. § 2721. |  | Signed into law on September 13, 1994. |
| ***Health Insurance Portability and Accountability Act (HIPAA),***Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164 | While the HIPAA Privacy Rule permits disclosure for treatment, payment, health care operations and in certain other exigent circumstances without an individual’s consent, it also provides that individuals must opt-in to disclosure of psychotherapy notes and marketing, and affords an opportunity to opt-out of facility directories, disclosure to caregivers, and certain other uses. All other uses require individual consent. |  | Signed into law on August 21, 1996. |
| 5 | ***V Choice***  **(Ref. Para. 26)**  Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be  appropriate for personal information controllers to provide these mechanisms when collecting publicly available information. | ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | Under the Communications Act, the customer may consent to the additional disclosure of his personal information by the telecommunications carrier beyond whatever disclosure is already permitted by law, 47 U.S.C. §§ 222(c)(1), 551(c)(1), including for the solicitation of additional services dissimilar to those which he already has, 47 U.S.C. § 551(c)(2)(C); 47 C.F.R. § 64.2005(b). In addition, a customer may affirmatively request in writing that a telecommunications carrier disclose personal information to a particular party. 47 U.S.C. § 222(c)(2). |  | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),*** 15 U.S.C. §§ 7701-7713, applicable to commercial electronic e-mail messages. | CAN-SPAM requires unsolicited commercial e-mail messages to be identified as solicitation and to include opt-out instructions and the sender's physical address. Senders must honor requests to opt-out within 10 business days. 15 U.S.C. §7704. |  | Signed into law on December 16, 2003. |
| ***Video Privacy Protection Act (VPPA),***18 U.S.C. § 2710, applicable to businesses that rent, sell or deliver pre-recorded videos. | Restricts businesses from disclosing personally identifiable video rental or purchase records without the consumer’s written consent. 18 U.S.C. § 2710(b). |  | Signed into law on November 5, 1998. |
| ***The Fair Credit Reporting Act (FCRA),*** 15 U.S.C. § 1681 et seq. | The FCRA includes accuracy requirements that apply to both consumer reporting agencies and furnishers of information to consumer reporting agencies. 15 U.S.C. §§ 1681e(b), 1681s-2(a)(1) 16 C.F.R. Part 660, 12 C.F.R. Part 1022, Subpart E.  The Dodd-Frank Act transferred to the Consumer Financial Protection Bureau most of the rulemaking responsibilities added to this Act by the Fair and Accurate Credit Transactions Act and the Credit CARD Act, but the FTC retains all its enforcement authority.  The FCRA provides for procedures allowing consumers to dispute information with con­sum­er reporting agencies, and requires the Consumer Financial Protection Bureau to promulgate regulations (12 CFR Subpart E) that identify the circumstances under which a furnisher is required to reinvestigate a dispute concerning the accuracy of information contained in a consumer report on the consumer, based on a direct request of a consumer. 15 U.S.C. § 1681i, 1681s-2(a)(8). ) 16 C.F.R. Part 660, 12 C.F.R. Part 1022, Subpart E.  The FCRA requires users of consumer reports to develop and implement reasonable policies and procedures to respond when they receive notices from consumer reporting agencies that the address of the consumer that the user provided to the consumer reporting agency to obtain a consumer report differs substantially from the address the consumer reporting agency has in its file. 15 U.S.C. § 1681c(h), 16 C.F.R. Part 641, 12 C.F.R. 1022, Subpart I. |  | Signed into law on October 26, 1970. |
| State defamation laws. (Statutory and common law) | Generally, state laws provide for tort claims for defamation -- an intentional false communication, either published or spoken, that injures another’s reputation or good name. |  |  |
| ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA mandates strong safeguards by requiring consumer reporting agencies to establish reasonable procedures to ensure that they provide data only to parties that have a “permissible purpose” for it. Specifically, agencies must verify the identity of each such party, and require it to certify the purposes for which information will be sought from the agency and that it will be used for no other purpose, before it provides any consumer reports to that party. 15 U.S.C. §§ 1681b(a), 1681e(a). The FCRA requires financial institutions and creditors to establish reasonable policies and procedures for implementing agency guidelines for identifying patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. 15 U.S.C. § 1681m(e), 16 C.F.R. Part 681. |  | Signed into law on October 26, 1970. |
| ***The Gramm-Leach-Bliley Act (GLBA),***Subchapter I (Disclosure of Nonpublic Personal Information) 15 U.S.C. § 6801 et seq. | As required by the GLBA, relevant regulatory authorities have promulgated standards for administrative, technical and physical safeguards to protect the security and confidentiality of customer records held by financial institutions. 15 U.S.C. § 6801(b), 6804(b)(2); 16 C.F.R. §§ 314.3-314.4; The federal banking agencies have issued Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice describing the appropriate elements of a financial institution’s response program, including customer notification procedures. 70 Fed. Reg. 15736 (March 29, 2005); 12 CFR 208; 12 CFR 225; 12 CFR 30; 12 CFR 364; 12 CFR 568; 12 CFR 570 |  | Signed into law on November 12, 1999. |
| ***The Children’s Online Privacy Protection Act (COPPA),***15 U.S.C. § 6501 et seq; 16 C.F.R. Part 312. | Under COPPA, covered operators must establish and maintain reasonable procedures to protect the confidentiality and security, and integrity of personal information collected from children. 15 U.S.C. § 6502(b)(1); 16 C.F.R. § 312.8. |  | Signed into law on October 21, 1998. |
| 6 | ***VI Integrity of Personal Information***  **(Ref. Para. 27)**  Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. | ***The Federal Trade Commission Act (FTC ACT),***15 U.S.C. § 41 et. seq. | The FTC Act prohibits deceptive data security practices, including the failure to provide reasonable security for consumer information, in violation of a privacy policy or representations. It also prohibits unfair data security practices that cause or are likely to cause substantial consumer injury which is not reasonably avoidable by consumers and which is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45. |  | Signed into law on September 26, 1914. |
| ***The Drivers Privacy Protection Act of 1994 (DPPA),***18 U.S.C. § 2721 et seq. | The DPPA’s permissible uses provisions necessitate strong security safeguards. 18 U.S.C. § 2721. |  | Signed into law on September 13, 1994. |
| ***Health Insurance Portability and Accountability Act (HIPAA),*** Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164 | The HIPAA Privacy Rule requires covered entities to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. It specifically requires safeguards that reasonably protect the health information from intentional or unintentional use of disclosure in violation of the rule, and that limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. 45 C.F.R. § 164.530. |  | Signed into law on August 21, 1996. |
| 7 | ***VII Security Safeguards***  **(Ref. Para. 28)**  Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. | ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | The Communications Act requires that telecommunications carriers have training and disciplinary procedures in place to prevent the disclosure of personal customer information that was not authorized by either law or customer consent. 47 C.F.R. § 64.2009(b). The Act also specifically requires that cable operators take such actions as are necessary to prevent unauthorized access to any personal customer information. 47 U.S.C. § 551(c). Moreover, cable operators are required to destroy any such information when it is no longer necessary for the purpose for which it was collected. 47 U.S.C. § 551(e). These cable requirements also apply to open video systems. 47 C.F.R. § 76.1510. |  | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Video Privacy Protection Act (VPPA),***18 U.S.C. § 2710, applicable to businesses that rent, sell or deliver pre-recorded videos. | The VPPA requires businesses to destroy personally identifiable rental information within a year after it is no longer required. 18 U.S.C. § 2710(e). |  | Signed into law on November 5, 1988. |
| ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA requires consumer reporting agencies to disclose to consum­ers most of their file information upon request, with a few exceptions. 15 U.S.C. § 1681g(a). In many cases, the disclosure is without charge. 15 U.S.C. § 1681j. In cases of disputed accuracy, the FCRA requires consumer reporting agen­cies and furnishers to reinvestigate information challenged by the consumer. 15 U.S.C. §§ 1681i, 1681s-2(b), 16 C.F.R. Part 660, 12 C.F.R. Part 1022, Subpart E. |  | Signed into law on October 26, 1970. |
| ***The Children’s Online Privacy Protection Act (COPPA),*** 15 U.S.C. § 6501 et seq; 16 C.F.R. Part 312. | COPPA provides parents with the right to review and delete the personal information provided by a child. 15 U.S.C. § 6502 (b)(1)(B); 16 C.F.R. §§ 312.3(c) and 312.6. |  | Signed into law on October 21, 1998. |
| ***Health Insurance Portability and Accountability Act (HIPAA),*** Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164. | The HIPAA Privacy Rule grants an individual the right to access, inspect, and obtain a copy of protected health information about themselves in a designated record set with narrow exceptions. The custodian is permitted to charge a reasonable fee. An individual has the right to request amendment of protected health information held by a covered entity in a designated record set with certain exceptions. The individual has the right to a timely written denial, and has the right to submit a statement of disagreement that must be placed in the record and disclosed with the record. The covered entity may include a rebuttal. 45 C.F.R. Part 164. |  | Signed into law on August 21, 1996. |
| ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | For cable operators in particular, the Communications Act provides for access to, and correction of, personal information by customers. 47 U.S.C. § 551(d). These requirements also apply to open video systems. 47 C.F.R. § 76.1510. |  | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Family Educational and Privacy Rights Act (FERPA),*** 20 U.S.C. § 1232g, applicable to all schools that receive funds under an applicable program of the U.S. Department of Education. | With certain limited exceptions, schools must allow a student (or the parent if the student is a minor) the opportunity to review and challenge or correct school records. 20 U.S.C. § 1232g(a). |  | Signed into law on August 21, 1974. |
| ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA provides for limited accountability by requiring prospective users of consumer report information to certify the purpose for which they seek to acquire the consumer report information and that they will use the information only for that purpose, and by prohibiting the release of consumer report information by a consumer reporting agency when information is sought for a non-permissible purpose. 15 U.S.C. § 1681e. |  | Signed into law on October 26, 1970. |
| 8 | ***VIII Access and Correction***  **(Ref. Para. 29-31)**  Individuals should be able to:  a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;  b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;  i. within a reasonable time;  ii. at a charge, if any, that is not excessive;  iii. in a reasonable manner;  iv. in a form that is generally understandable; and,  c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.  Such access and opportunity for correction should be provided except where:  (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question;  (ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or  (iii) the information privacy of persons other than the individual would be violated.  If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial. | ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA requires consumer reporting agencies to disclose to consum­ers most of their file information upon request, with a few exceptions. 15 U.S.C. § 1681g(a). In many cases, the disclosure is without charge. 15 U.S.C. § 1681j. In cases of disputed accuracy, the FCRA requires consumer reporting agen­cies and furnishers to reinvestigate information challenged by the consumer. 15 U.S.C. §§ 1681i, 1681s-2(b), 16 C.F.R. Part 660, 12 C.F.R. Part 1022, Subpart E. |  | Signed into law on October 26, 1970. |
| ***The Children’s Online Privacy Protection Act (COPPA),*** 15 U.S.C. § 6501 et seq; 16 C.F.R. Part 312. | COPPA provides parents with the right to review and delete the personal information provided by a child. 15 U.S.C. § 6502 (b)(1)(B); 16 C.F.R. §§ 312.3(c) and 312.6. |  | Signed into law on October 21, 1998. |
| ***Health Insurance Portability and Accountability Act (HIPAA),*** Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164. | The HIPAA Privacy Rule grants an individual the right to access, inspect, and obtain a copy of protected health information about themselves in a designated record set with narrow exceptions. The custodian is permitted to charge a reasonable fee. An individual has the right to request amendment of protected health information held by a covered entity in a designated record set with certain exceptions. The individual has the right to a timely written denial, and has the right to submit a statement of disagreement that must be placed in the record and disclosed with the record. The covered entity may include a rebuttal. 45 C.F.R. Part 164. |  | Signed into law on August 21, 1996. |
| ***Communications Act of 1934 (as amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996),*** 47 U.S.C. § 151 et seq. | For cable operators in particular, the Communications Act provides for access to, and correction of, personal information by customers. 47 U.S.C. § 551(d). These requirements also apply to open video systems. 47 C.F.R. § 76.1510. |  | Signed into law on June 19, 1934. Amended by the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996. |
| ***Family Educational and Privacy Rights Act (FERPA),*** 20 U.S.C. § 1232g, applicable to all schools that receive funds under an applicable program of the U.S. Department of Education. | With certain limited exceptions, schools must allow a student (or the parent if the student is a minor) the opportunity to review and challenge or correct school records. 20 U.S.C. § 1232g(a). |  | Signed into law on August 21, 1974. |
| 9 | ***IX Accountability***  **(Ref. Para. 32)**  A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.  When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. | ***The Fair Credit Reporting Act (FCRA),***15 U.S.C. § 1681 et seq. | The FCRA provides for limited accountability by requiring prospective users of consumer report information to certify the purpose for which they seek to acquire the consumer report information and that they will use the information only for that purpose, and by prohibiting the release of consumer report information by a consumer reporting agency when information is sought for a non-permissible purpose. 15 U.S.C. § 1681e. |  | Signed into law on October 26, 1970. |
| ***The Gramm-Leach-Bliley Act (GLBA),***Subchapter I (Disclosure of Nonpublic Personal Information) 15 U.S.C. § 6801 et seq. | The GLBA creates accountability for covered entities by requiring them to ensure that their own affiliates as well as any third-party service providers with access to customer information maintain appropriate safeguards. 16 C.F.R. 314.2, 314.4. |  | Signed into law on November 12, 1999. |
| ***The Federal Trade Commission Act (FTC ACT),***15 U.S.C. § 41 et. seq. | Section 5 of the FTC Act prohibits “deceptive” or “unfair” practices, such as a business’s false promise that it will disclose information to third-party service providers only to the extent necessary to perform services on behalf of the business, or a service provider’s practice of collecting and sharing personal information in a way that contradicts merchants’ privacy policies. 15 U.S.C. § 45. |  | Signed into law on September 26, 1914. |
| ***The Drivers Privacy Protection Act of 1994 (DPPA),*** 18 U.S.C. § 2721 et seq. | The DPPA provides for limited accountability by prohibiting state motor vehicle departments from disclosing an individual’s personal information outside of a permissible use and by requiring state motor vehicle departments to obtain a waiver from the individual before releasing the individual’s personal information for requests outside of the permissible uses. Further, authorized recipients of personal information may not resell or redisclose the personal information outside of the permissible uses except when the individual has consented and must keep records regarding any such resale or redisclosure. 18 U.S.C. §§ 2721(c), 2721(d). |  | Signed into law on September 13, 1994. |
| ***Health Insurance Portability and Accountability Act (HIPAA),***Pub. L. 104-191 §§ 262 & 264) Privacy Rule, 45 C.F.R. Parts 160 & 164. | Under the HIPAA Rule, a covered entity must enter into agreements with its business associates to whom protected health information is disclosed requiring appropriate safeguards. Covered entities may be criminally and civilly liable for disclosures in violation of the Privacy Rule. 45 C.F.R. Part 164. |  | Signed into law on August 21, 1996. |

-- // --

1. *Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.* [↑](#footnote-ref-2)
2. *Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled “APEC Principle/ Commentary”.* [↑](#footnote-ref-3)
3. *Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).*  [↑](#footnote-ref-4)
4. *Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies’ practice, for example enacted, introduced, draft.  If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."* [↑](#footnote-ref-5)
5. <https://www.consumerfinance.gov/rules-policy/regulations/1016/1/#b-1> [↑](#footnote-ref-6)
6. <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm> [↑](#footnote-ref-7)