

## **An Overview of Federal Privacy-Related Regulations in the United States**

In the United States, there are a number of Federal laws that contain provisions that protect consumers in the privacy area<sup>1</sup>. They include:

### ***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 and deceptive” business practices. The FTC uses this broad authority to protect consumer privacy interests where deceptive and unfair business practices result in harmful privacy violations.
- 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 change a privacy policy and then retroactively apply the new policy to information collected under the earlier policy.
- 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 substantial consumer injury without offsetting benefits.
- Under Section 5 of the FTC Act, a business that shares consumer information with a service provider is responsible for ensuring that the service provider treats the information in accordance with the laws applicable to the company that is sharing the information. 15 U.S.C. § 45.
- For violations of Section 5 of the FTC Act, the FTC may obtain injunctive relief, monetary remedies in the form of consumer redress and disgorgement of illicit gains, and other appropriate equitable relief. 15 U.S.C. § 53(b). 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.

### ***The Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.***

- The FCRA protects 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

---

<sup>1</sup> SOURCE: United States Individual Action Plan (IAP) Submission to the Asia Pacific Economic Cooperation (APEC), August, 2006.

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 those who procure 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), 1681e(b), 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. Moreover, creditors and depository institutions must implement policies and procedures to identify and mitigate against identity theft. 15 U.S.C. § 1681m(e).
- 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). Creditors 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). 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. 15 U.S.C. §1681m. 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).
- 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 transactions. 15 U.S.C. § 1681c(a). Also, the FCRA requires businesses that obtain any compilation of consumer information to dispose of the information to prevent its subsequent use for improper purposes. 15 U.S.C. § 1681w, 16 C.F.R. Part 682.
- 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); 70 Fed. Reg. 70664 (Nov. 22, 2005).

- 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” if the consumer gives his or her consent. 15 U.S.C. § 1681b(a)(2). 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. 1681s-3.
- 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, 1681s-2(a)(1). Similarly, it provides for procedures allowing consumers to dispute information with both consumer reporting agencies and furnishers. 15 U.S.C. § 1681i, 1681s-2(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).
- 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).
- The FCRA requires consumer reporting agencies to disclose to consumers all their file information upon request. 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 to reinvestigate information challenged by the consumer. 15 U.S.C. § 1681i.

- 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.
- 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 federal and state authorities as well as private litigants. It allows courts to impose penalties of up to \$2500 per knowing violation in actions brought by the FTC. 15 U.S.C. § 1681s(a).

***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)***

- The GLBA requires the FTC, along with the Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, the Commodity Futures Trading Commission 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. [NOTE: (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 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. 15 U.S.C. § 6803; 16 C.F.R. 313.4, 313.5, 313.6; 313.13.
- Under the GLBA, financial institutions must disclose in their privacy notices each category of information collected from and about consumers. Financial institutions must follow their stated practices and may only disclose the

- Under the GLBA, financial institutions must disclose in their privacy notices each category of information collected from and about consumers. 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. In addition, companies that receive consumers' personal information from a financial institution may only use or disclose that information consistent with the purposes for which they received it. 15 U.S.C. § 6802(c); 16 C.F.R. § 313.11.
- 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); 16 C.F.R. 314; 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).
- The GLBA, generally, allows consumers to opt out of the sharing of their information with third parties for marketing purposes. 15 U.S.C. § 6802(b); 16 C.F.R. 313.7, 313.10, cf. 313.13 (providing for a joint-marketing exception).
- 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.
- 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 Section 5 of the FTC Act, including injunctive relief, monetary remedies in the forms of consumer redress and disgorgement of illicit gains, and other appropriate monetary relief. 15 U.S.C. § 53(b); 15 U.S.C. §§ 6805, 6822. In addition, obtaining customer information by false pretenses may carry criminal penalties. 15 U.S.C. § 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.

***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.***

- The COPPA applies to operators of Web sites 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.
- The COPPA requires operators to post notice of their information practices on their Web site 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.
- The COPPA 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. The COPPA also requires parental consent for the collection, use and disclosure of personal information from children. 15 U.S.C. §§ 6501 and 6502(b)(1); 16 C.F.R. §§ 312.3 and 312.7.
- The 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. The representations in an operator's notice and the scope of parental consent are binding on the operator. 15 U.S.C. § 6502(b)(1); 16 C.F.R. §§ 312.3, 312.4, 312.5.
- The 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.
- Under the COPPA, operators must establish and maintain reasonable procedures to protect the confidentiality and security of children's personal information. 15 U.S.C. § 6502(b)(1)(D); 16 C.F.R. 312.8.
- COPPA provides parents with the right to review and delete the personal information provided by a child. 15 U.S.C. § 6502(a)(2) and (b)(1)(B); 16 C.F.R. 312.3(c) and 312.6.
- The 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.

***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 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.
- 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.
- 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.
- 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.
- 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 or 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.

- 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.
- 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.

***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.
- 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. As well, customers shall 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. Cable customers shall also 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.
- 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),

- 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).
- 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.
- 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.
- 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.

***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.
- 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.
- 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.
- 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. Senders include the originator of the message and the person whose product, service or website is promoted by the advertisement. 15 U.S.C. § 7702(16).
- 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.

***Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 et seq.***

- ECPA requires that any person, with certain exceptions, is prohibited from intercepting electronic communications without the consent of at least one party to the communication. 18 U.S.C. § 2511.
- ECPA requires that any person, with certain exceptions, is prohibited from disclosing 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. Certain violations may carry criminal liability.

***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 re-disclosure 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.
- The DPPA limits the use of individuals' information to certain "permissible purposes" unless the individual consents to different uses. 18 U.S.C. § 2721.
- The DPPA provides for the disclosure and use of individuals' personal information other than for a "permissible purpose" if the individual gives his or her consent. 18 U.S.C. § 2721.
- The DPPA's permissible purposes provisions necessitate strong security safeguards. 18 U.S.C. § 2721.
- The DPPA provides for limited accountability by prohibiting state motor vehicle departments from disclosing an individual's personal information outside of a permissible purpose 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 purposes. Further, authorized recipients of personal information may not resell or re-disclose the personal information outside of the permissible purposes except when the individual has consented and must keep records regarding any such resale or re-disclosure. 18 U.S.C. §§ 2721(c), 2721(d).
- The 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.

***Family Educational and Privacy Rights Act (FERPA), 20 U.S.C. § 1232g***

- The FERPA is 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).
- 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).
- 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).

- Entities that violate FERPA are not eligible for funding from the applicable program.

***Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710***

- The VPPA is applicable to businesses that rent, sell or deliver pre-recorded videos and restricts businesses from disclosing personally identifiable video rental or purchase records without the consumer's written consent. 18 U.S.C. § 2710(b).
- 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).
- 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).

***Disclaimer***

This document does not purport to provide a complete picture of privacy protections available to consumers in the United States, as it does not include state laws and the numerous self-regulatory codes that could apply in electronic commerce. In addition, the summaries included in this document are not necessarily comprehensive; nor do they include all applicable exceptions to general rules. They are not intended to be relied on as legal advice and should not be used as statements of law in the context of legal proceedings. This document is not an official US government document, nor is it an official document of any US government branch or agency.