PERMANENT COUNCIL OF THE
ORGANIZATION OF AMERICAN STATES

COMMITTEE ON POLITICAL AND JURIDICAL AFFAIRS

OEA/Ser.G
CP/CAJP-3026/11 add. 9
5 March 2012
TEXTUAL

QUESTIONNAIRE REGARDING PRIVACY AND DATA PROTECTION LEGISLATION AND PRACTICES

[AG/RES. 2661 (XLI-O/11)]

(Answers by Member States: United States)

QUESTIONNAIRE REGARDING
PRIVACY AND DATA PROTECTION LEGISLATION AND PRACTICES

[AG/RES. 2661 (XLI-O/11)]

(Answers by Member States: United States)

QUESTIONNAIRE RESPONSES ON BEHALF OF THE UNITED STATES

I. LEGISLATION

A. Does your country's domestic legal system include (comprehensive or sectoral) privacy/data protection laws or regulations at the national/federal level? If so, please describe the laws or regulations briefly, including whether they apply to the private and/or public sector contexts, and attach copies of the provisions and the documents containing them.

The United States has enacted a number of sectoral laws at the federal level. These questionnaire responses will focus on those implicating the private or commercial sector rather than governmental use of personal data.[1/]

The U.S. Federal Trade Commission has broad authority in the commercial privacy area,[2/] including the enforcement of the following laws:

The Federal Trade Commission Act (FTC Act).[3/] 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. For violations of Section 5 of the FTC Act, the FTC may obtain injunctive relief,

---

1. With respect to governmental use of personal data, the International Association of Privacy Professionals offers a privacy professional's certification examination specializing in governmental use of personal data and provides a helpful listing of most of the main laws governing this area; see https://www.privacyassociation.org/images/uploads/CIPP_G_BoK_01_2012.pdf . The Privacy Act of 1974 is one of the primary federal laws protecting the privacy of information in the federal public sector. The Privacy Act was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow "fair information practice principles when gathering and handling personal data." Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it lets individuals sue the government for violating its provisions. The Privacy Act requires that information about an individual be relevant to and necessary for a required agency purpose and be sufficiently accurate, timely and complete to ensure fairness and limits agency uses of information to employees and officials with a need to know. For an overview of the U.S. Privacy Act of 1974, which governs primarily the U.S. Federal Executive Branch, see http://www.justice.gov/opcl/1974privacyact-overview.htm.

2. However, the FTC may not enforce laws against certain types of entities, such as banks. To the extent that enforcement authority is not assigned to the FTC, enforcement authority is assigned to another federal agency, such as an appropriate federal banking agency.

3. 15 U.S.C. § 41 et. seq., available online at XXX.

monetary remedies in the form of consumer redress and disgorgement of ill-gotten gains, and other appropriate equitable relief.[4/]

The Fair Credit Reporting Act (FCRA).[5/] The FCRA protects information collected by consumer reporting agencies, such as credit bureaus, medical information companies and tenant and employment screening services. A consumer reporting agency is not allowed to provide information in a consumer report to any person who does not have a purpose to use the information permitted under the Act. Also, a person who uses a consumer report for credit, insurance, or employment purposes must notify the consumer when an adverse action is taken on the basis of such a report. Further, users must identify the consumer reporting agency that provided the report, so that the accuracy and completeness of the report may be verified or contested by the consumer. The FCRA also regulates companies that provide information to consumer reporting agencies by imposing specific legal duties regarding the accuracy of the information, including the duty to investigate disputed information. The Fair and Accurate Credit Transactions Act**,** the Credit CARD Act and Dodd-Frank Act made a number of substantial changes to this Act.

The Gramm-Leach-Bliley Act (GLB).[6/] Title V, subtitle A, of the GLB Act is designed to ensure that financial institutions protect the privacy of nonpublic personal information about consumers. In general, the GLB Act, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act, authorizes the Bureau of Consumer Financial Protection (Bureau)[7/] to issue regulations governing the limitations on disclosures of nonpublic personal information by a financial institution to an unaffiliated third party. Under the GLB Act and the Bureau's privacy regulation, a financial institution must develop and give notice of its privacy policies to its own customers at least annually. In addition, the financial institution may not disclose any nonpublic personal information about a consumer to an unaffiliated third party, unless the institution first (1) provides its privacy notice to the consumer and (2) gives the consumer an opportunity to "opt out" from such disclosure, and the consumer does not opt out. The GLB Act also expressly limits the sharing of an account number for marketing purposes. Subtitle A of Title V also requires the FTC and other agencies to issue regulations (*see, e.g.*, 16 CFR Part 314) that require financial institutions to protect nonpublic personal information. Subtitle B of Title V prohibits obtaining customer information of a financial institution by false pretenses. In general, the FTC enforces the provisions of Title V of the GLB Act with regard to entities not specifically assigned by the provision to the Bureau, the Federal banking agencies, or other regulators.

The Children's Online Privacy Protection Act (COPPA).[8/] This Act protects children's privacy by giving parents the tools to control what information is collected from their children online. Under the Act's implementing Rule[9/], operators of commercial websites and online services directed to or

---

4 15 U.S.C. § 53(b).

5 15 U.S.C. § 1681 et seq. as amended, available at http://www.ftc.gov/os/statutes/031224fcra.pdf.

6 Pub. L.106-102, 113 Stat.1338, codified in relevant part at 15 U.S.C. §§ 6801-6809 and §§ 6821-6827, as amended; available at http://www.law.cornell.edu/uscode/uscode15/usc_sec_15_00006801----000-.html.

7 The GLB Act also grants authority to the Federal Trade Commission (FTC) to issue rules for certain nonbank financial institutions, as well as authority to the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) to issue rules that apply to the financial institutions that are subject to the jurisdiction of those agencies, respectively. The CFTC, FTC, and SEC are in charge of enforcing their own privacy rules under the GLB Act.

8 15 U.S.C. §§ 6501-6506; see http://www.ftc.gov/privacy/coppafaqs.shtm.

9 Codified at 16 C.F.R. Part 312.

knowingly collecting personal information from children under 13 must: (1) notify parents of their information practices; (2) obtain verifiable parental consent before collecting a child's personal information; (3) give parents a choice as to whether their child's information will be disclosed to third parties; (4) provide parents access to their child's information; (5) let parents prevent further use of collected information; (6) not require a child to provide more information than is reasonably necessary to participate in an activity; and (7) maintain the confidentiality, security, and integrity of the information.

The Telemarketing and Consumer Fraud and Abuse Prevention Act.[10/] This Act requires the U.S. Federal Trade Commission (FTC) to promulgate regulations (1) defining and prohibiting deceptive telemarketing acts or practices; (2) prohibiting telemarketers from engaging in a pattern of unsolicited telephone calls that a reasonable consumer would consider coercive or an invasion of privacy; (3) restricting the hours of the day and night when unsolicited telephone calls may be made to consumers; and (4) requiring disclosure of the nature of the call at the start of an unsolicited call made to sell goods or services. The law expressly authorizes the FTC to include within the rules' coverage entities that "assist or facilitate" deceptive telemarketing practices.

The Do-Not Call Registry Act of 2003 (15 U.S.C. § 6151; originally codified at 15 U.S.C. § 6101 note) expressly authorized the FTC under section 3(a)(3)(A) of the Telemarketing and Consumer Fraud and Abuse Prevention Act to implement and enforce a Do-Not-Call Registry, which protects consumer privacy by allowing consumers to avoid telemarketing calls from businesses. The FTC and the Federal Communications Commission (FCC) jointly monitor compliance with the Do-Not-Call Registry.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) (15 U.S.C §§ 7701-7713). This Act establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial email provide recipients with a method for opting out of receiving such email and must be identified as an advertisement. The FTC enforces the provisions of the CAN SPAM Act jointly with the FCC.

Other privacy-related laws governing the private sector that do not fall under the FTC's jurisdiction include but are not limited to the following:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the implementing regulations issued by the U.S. Department of Health and Human Services (the "Privacy Rule" and the "Security Rule").[11/] HIPAA provides federal protections for personal health information held by covered entities. "Covered entities" include health care providers, health plans, and health care clearinghouses. HIPAA applies to both public and private sector covered entities. The HIPAA Privacy Rule regulates the uses and disclosures covered entities may make of individually identifiable health information, requires the information be safeguarded, and gives individuals rights

10 Codified in relevant part at 15 U.S.C. §§ 6101-6108; available at http://www.law.cornell.edu/uscode/15/ch87.html. The FTC's rules can be found at 16 C.F.R. Part 310.
11 Public Law 104-191; HHS regulations at 45 C.F.R. Parts 160 and 164; copies available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.

with respect to their health information, including rights to examine and obtain a copy of their health records and to request corrections. The HIPAA Security Rule requires covered entities to implement a series of administrative, physical, and technical safeguards to assure the confidentiality, integrity, and availability of electronic protected health information. In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act, strengthened HIPAA's privacy and security protections by, among other provisions, extending certain requirements of the rules directly to contractors of covered entities that handle personal health information.

Health Information Breach Notification Rule (Health and Human Services).[12/] Covered entities are required to provide notice to patients, HHS, and in some cases, the media following a breach of unsecured protected health information. Contractors of covered entities are also required to notify covered entities following the discovery of such a breach.

Health Breach Notification Rule (Federal Trade Commission).[13/] Vendors of personal health records (PHRs) and related entities are required to provide notice to consumers following a breach of unsecured, individually identifiable electronic health information. If a third-party service provider of a PHR vendor experiences a breach, it must notify the PHR vendor. The PHR vendor, in turn, must notify each affected person who is a citizen or resident of the United States, the Federal Trade Commission and in some cases, the media.

The Americans with Disabilities Act (ADA).[14/] The ADA generally prohibits prospective employers from conducting a medical examination or making inquiries of a job applicant as to whether such applicant is an individual with a disability or as to the nature or severity of such disability, except where the inquiry is job-related and consistent with business necessity. The Equal Employment Opportunity Commission (EEOC) has issued implementing regulations that provide that information collected regarding the medical condition or history of a job applicant must be collected and maintained on separate forms and in separate medical files and be treated as a confidential medical record.[15/] The EEOC issues additional guidance on employment-related inquiries.[16/]

The Genetic Information Nondiscrimination Act (GINA).[17/] GINA generally prohibits discrimination based on an individual's genetic information with respect to both health coverage and employment. Title I of GINA generally prohibits discrimination in group premiums based on genetic information, proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental policy (Medigap) insurance markets, and limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing. In addition to the nondiscrimination

---

12 45 CFR Part 160 and 45 CFR Part 164 Subparts A and D, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
13 16 CFR Part 318, available at http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule.
14 Pub. L. 101-336, as amended. Titles I and V of the ADA are online at http://www.eeoc.gov/laws/statutes/ada.cfm.
15 29 C.F.R. Part 1630, available at http://www.gpo.gov/fdsys/pkg/CFR-2011-title29-vol4/xml/CFR-2011-title29-vol4-part1630.xml; *see* in particular 29 C.F.R. § 1630.14(b)(1).
16 See, e.g., Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations, EEOC NOTICE Number 915.002, 10/10/9, available at http://www.eeoc.gov/policy/docs/preemp.html.
17 Available at http://www.eeoc.gov/laws/statutes/gina.cfm.

provisions, Title II of GINA prohibits the use of genetic information in making employment decisions and limits employer access to genetic information. The Act also imposes confidentiality obligations on employers and other covered entities (employment agencies, labor unions, and training programs) that possess genetic information. Its implementing regulations are issued by the EEOC, HHS, the Department of the Treasury, and the U.S. Department of Labor.[18/]

Title X of the Public Health Service Act, Confidentiality of Title X Service Information.[19/] Title X of the Public Health Services Act provides funding for family planning. The statutes and regulations implementing the Title X program contain consent and confidentiality rules designed to reduce barriers to health care and to protect the privacy of adolescent service recipients.

Title X regulations require that Title X-funded providers keep confidential "all information as to personal facts and circumstances [about patients] obtained by the project staff." The regulations prohibit providers from releasing a patient's individual information unless the provider has written authorization for the release, the release is necessary to provide services to the patient, or state or federal law requires the release. The regulations also require that providers implement "appropriate safeguards for confidentiality." Otherwise, information may be disclosed only in summary, statistical, or other form which does not identify particular individuals.

SAMHSA: Confidentiality of Substance Abuse Patient Records.[20/] These regulations prohibit substance abuse and alcohol treatment facilities that receive federal support from disclosing patient records that would identify a patient as an alcohol or drug abuser without the patient's express, specific consent. The protection generally follows the data and recipients are prohibited from further disclosing the data without obtaining additional permission from the patient.

Medicaid Privacy Requirements.[21/] The federal Medicaid confidential data standard is established by §1902(a)(7) of the Social Security Act (42 USC § 1396a(a)(7)). The law requires that a "State plan for medical assistance must: (7) provide safeguards which restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan." This statutory requirement is implemented in regulations at 42 CFR § 431.300 et seq.

Federal Food, Drug and Cosmetic Act (FDCA).[22/] No investigator may involve a human being as a subject in research covered by these regulations unless the investigator has obtained the legally effective informed consent of the subject or the subject's legally authorized representative. An investigator shall seek such consent only under circumstances that provide the prospective subject or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence. In seeking informed consent a statement shall be provided to each subject describing the extent, if any, to which confidentiality of records identifying

---

18 See http://www.eeoc.gov/laws/types/genetic.cfm. Public Law 110-233, 122 Stat. 881, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ233.110.pdf
19 42 C.F.R. § 59.11, available at http://law.justia.com/cfr/title42/42-1.0.1.4.41.1.19.11.html.
20 42 CFR Part 2 and 42 USC § 290-dd-2, available at http://www.samhsa.gov/legislate/Sept01/01907_42cfr_part2.htm.
21 42 CFR §§ 431.300-307 and 42 USC 1396a(a)(7), available at https://www.emedny.org/epaces/MedConfidentialityReg.aspx#Question_1.
22 21 CFR Part 50 available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=50.

the subject will be maintained and that notes the possibility that the Food and Drug Administration may inspect the records.

Controlled Substances Act (CSA).[23/] CSA protects identifiable research information from forced or compelled disclosure. CSA allows for refusal to disclose identifying information regarding research participants in civil, criminal, administrative, legislative, or other proceedings.

Federal Policy for the Protection of Human Subjects (Common Rule).[24/] The U.S. Department of Health and Human Services (HHS) has federal regulations governing the protection of human subjects in research which include provisions related to protecting the privacy of research subjects and maintaining the confidentiality of research data. Specifically, 45 CFR 46.111(a)(7) requires that in order to approve a research study, an institutional review board (IRB) must determine that, "when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data." In addition, the HHS regulations also require that subjects be informed of "the extent, if any, to which the confidentiality of records identifying the subject will be maintained," unless an IRB has waived the requirement for informed consent (45 CFR 46.116((a)(5)).

The HHS regulations for the protection of human subjects apply to any institution engaged in non-exempt human subjects research that is conducted or supported by HHS. In addition, the HHS regulations also apply to non-exempt human subjects research, that is *not* conducted or supported by HHS, if the research is conducted by a U.S. institution that has voluntarily elected to comply with the HHS regulations (through an assurance document approved by the HHS Office for Human Research Protections) for all the research conducted at the institution. However, such extension of the HHS regulations is not required.

In addition to HHS, 14 other U.S. Federal departments and agencies adopted a uniform set of rules for the protection of human subjects.[25/]

Statutory Authority for Certificates of Confidentiality.[26/] Under section 301(d) of the Public Health Service Act (42 U.S.C. 241(d)) the Secretary of Health and Human Services may authorize persons engaged in biomedical, behavioral, clinical, or other research to protect the privacy of individuals who are the subjects of that research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons authorized by the National Institutes of Health (NIH) to protect the privacy of research subjects may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify them by name or other identifying characteristic.

Certificates can be used for biomedical, behavioral, clinical or other types of research that is sensitive, which means that disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation.

---

23 21 CFR § 1316.23 and 21 USC § 801, available at http://www.deadiversion.usdoj.gov/21cfr/cfr/1316/1316_23.htm and http://www.deadiversion.usdoj.gov/21cfr/21usc/801.htm.
2445 CFR § 46 subparts A through E; Specifically 45 CFR § 46.111(a)(7) and 45 CFR § 46.116(a)(5), available at http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html.
25 http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html.
26 42 U.S.C. 241(d), available at http://www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000241----000-.html.

Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act).[27/] The Patient Safety Act establishes a voluntary reporting system for hospitals, doctors and other health care providers to provide information related to patient safety events which will be aggregated and analyzed to assess and resolve patient safety and health care quality issues. To encourage the reporting and analysis of medical errors, the Patient Safety Act provides Federal privilege and confidentiality protections for patient safety information called *patient safety work product*. Patient safety work product includes information collected and created during the reporting and analysis of patient safety events.
The confidentiality provisions will improve patient safety outcomes by creating an environment where providers may report and examine patient safety events without fear of increased liability risk. Greater reporting and analysis of patient safety events will yield increased data and better understanding of patient safety events.

Fair Credit Reporting Medical Information Regulations (2005).[28/] A creditor may not obtain or use medical information in connection with any determination of a consumer's eligibility, or continued eligibility, for credit, except as permitted by the Fair and Accurate Credit Transactions Act (FACT). In general a creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as: (i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds; (ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and (iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

AHRQ Confidentiality Provisions.[29/] AHRQ cannot use data it collects for any purpose other than the purpose for which it was supplied unless the identifiable establishment, person, or other supplier of the data has consented to its use for such other purpose. Individuals who violate this provision are subject to a civil penalty of up to $10,000.

CDC Confidentiality Provisions.[30/] Identifiable information or data must be used for the purpose for which it was supplied unless the establishment or person identified by the data has consented, as determined under regulations of the Secretary, to its use for another purpose.

The Communications Act of 1934, as amended. [31/]The Communications Act, as enforced by the Federal Communications Commission, protects the privacy and security of consumer information collected by communications providers in the operation of their networks, including telecommunications carriers, interconnected Voice over Internet Protocol (VoIP) providers, cable operators and satellite operators. The Act imposes a duty on these communications providers to

---

27 42 U.S.C. § 299b-21 to 299b-26 and Public Law 109-41 109th Congress, available at http://codes.lp.findlaw.com/uscode/42/6A/VII/C/299b-21 and http://www.pso.ahrq.gov/statute/pl109-41.htm (public law).
28 12 CFR Part 717, available at http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr717_06.html.
29 42 U.S.C. § 299c-3(d) available at http://codes.lp.findlaw.com/uscode/42/6A/VII/D/299c-3. See also http://www.ahrq.gov/fund/datamemo.htm.
30 42 U.S.C. § 242m(d) available at http://www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000242---m000-.html.
31 47 U.S.C. § 151 et seq., available at http://transition.fcc.gov/telecom.html.

protect the confidentiality of customers' personal information, and limits the power of such entities to use or disclose that information.[32/] In addition, the FCC has a caller identification ("caller ID") privacy requirement that prohibits common carriers from passing the calling party number to the called party where a privacy request has been made by the caller.[33/] The Act also prohibits unauthorized interception and publication of communications made by wire or radio.

Telephone Consumer Protection Act (TCPA), [34/]as amended by the Junk Fax Prevention Act (Junk Fax Act)[35/] nd the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act.[36/] These statutes protect consumers from unwanted telephone solicitations, unsolicited faxes, and unwanted commercial email messages, respectively. Under the TCPA, the FCC limits telephone solicitation calls to residential phone numbers, for example by prohibiting telephone solicitation calls before 8:00 am or after 9:00 pm and requiring telemarketers to comply with do-not-call requests. The TCPA and FCC rules also prohibit sending unwanted prerecorded or autodialed voice calls or text messages, regardless of content, to any wireless phone without the recipient's consent, and prohibit sending prerecorded telemarketing calls to a residential number without the recipient's consent. The Junk Fax Act prohibits most unsolicited fax advertisements without the recipient's prior express invitation or permission, unless the sender has a prior established business relationship with the recipient, and requires that all fax advertisements contain a clear and conspicuous opt-out option for the recipient. The CAN-SPAM Act prohibits sending unwanted commercial email messages to wireless devices without prior permission. The FCC jointly enforces these statutory provisions with the FTC.[37/]

The Drivers Privacy Protection Act of 1994 (DPPA).[38/]The DPPA protects individuals' personal information collected by state departments of motor vehicles. It limits the disclosure of such personal information to certain "permissible uses", and requires individual consent for any re-sale and re-disclosure of such information by authorized users, including businesses, for purposes other than the "permissible uses."

Electronic Communications Privacy Act (ECPA).[39/] ECPA addresses, *inter alia*, access to stored wire and electronic communications and transactional records, and the use of pen registers and trap and trace devices. The Act generally prohibits unauthorized access to or disclosure of stored wire and electronic communications in specified cases; it also provides for legal procedures that law enforcement may use to obtain such communications and records. The pen register and trap and trace provisions prohibit the installation or use of a pen register or trap and trade device, except as provided for in the statute. Except in narrow circumstances, law enforcement may not install a pen register or a trap and trace device without a prior court order.

---

32 47 U.S.C. §§ 222, 338(i), 551.
33 *See* 47 C.F.R. § 64.1601(b).
34 Codified as 47 U.S.C. § 227.
35 *Id.*
36 15 U.S.C. 7701, et seq., Public Law No. 108-187.
37 The FTC also administers a national Do-Not-Call registry that allows consumers to limit the telemarketing calls they receive. The Do-Not-Call registry is enforced by the FTC, FCC and state law enforcement officials.
38 18 U.S.C. § 2721 et seq.
39 Codified at 20 U.S.C. § 1232g *et seq.*); 34 C.F.R. part 99 (implementing FERPA). *See also* Individuals with Disabilities Education Act of 1970 (IDEA), as revised generally by the Individuals with Disabilities Education Improvement Act of 2004, Title I of Pub. L. 108-446 (codified at 20 U.S.C. § 1400 *et seq*.), particularly 20 U.S.C. § 1412(a)(8).

Family Educational and Privacy Rights Act (FERPA).[40/] FERPA applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education. It protects the privacy of students' education records by requiring that recipient schools may not have a policy or practice of denying parents the right to inspect and review education records within 45 days of a request or to seek to amend education records believed to be inaccurate. Parents also have the right under FERPA to consent to the disclosure of personally identifiable information from education records, except as specified by law. These rights transfer to the student when he or she turns 18 years of age or enters a postsecondary educational institution at any age ("eligible student").

Protection of Pupil Rights Amendment (PPRA).[41/] The PPRA provides parents with certain rights relative to a survey, analysis, or evaluation given to students that concerns one or more of eight protected areas, including illegal, anti-social, self-incriminating, or demeaning behavior, sex behavior or attitudes, or political affiliations or beliefs of the student or the student's family. For U.S. Department of Education funded surveys, parents have the right to inspect and review the survey and provide consent before students can be required to take the survey. For surveys not funded by the Department but given by schools that receive funds from the Department under other programs, schools must provide parents with an opportunity to inspect and review the survey and an opportunity to opt their children out of participation. PPRA also concerns marketing surveys and other areas of student privacy, parental access to information, and the administration of certain physical examinations to minors. The rights under PPRA transfer from the parents to a student who is 18 years old or an emancipated minor under State law.

Video Privacy Protection Act (VPPA).[42/] The VPPA applies to businesses that rent, sell or deliver pre-recorded videos. It restricts businesses from disclosing personally identifiable video rental or purchase records without the consumer's written consent. It requires businesses to destroy personally identifiable rental information within a year after it is no longer required.

On February 23, 2012, the Obama Administration released a White Paper on commercial data privacy articulating a Consumer Privacy Bill of Rights.[43/] The White Paper calls upon Congress to codify the Consumer Privacy Bill of Rights and give both the FTC and state-level Attorneys General the power to enforce these rights directly. The White Paper also calls for a national standard for data breach notification that would preempt state legislation.[44/]

---

40 20 U.S.C. § 1232g.
41 20 U.S.C. § 1232h; 34 CFR part 98.
42 18 U.S.C. § 2710.
43 "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("White Paper").
44 White Paper, at pp. 35-39.

B. Does your country's domestic legal system include (comprehensive or sectoral) privacy/data protection laws or regulations at the state/municipal/local level? If so, please describe the laws or regulations briefly and attach copies of the provisions and the documents containing them.

A number of States have adopted laws related to data privacy and 47 States, the District of Columbia, and several U.S. Territories have data breach notification laws. A list of a number of the privacy laws, with links where available, is provided below.[45/]

Privacy-related State Laws (Sampling) from NCSL website
Minnesota statutes on internet privacy §§ 325M.01 to .09
Nevada statute on privacy requirements for internet service providers § 205.498
California requirements on disclosures for third party sharing §§ 1798.83 to .84
California's Online Privacy Protection Act §§ 22575-22578
Utah requirements on disclosures for third party sharing §§ 13-37-101, -102, -201, -202, -203
Delaware requirements for employer notice of email/Internet monitoring § 19-7-705
Connecticut requirements for employer notice of electronic monitoring § 31-48d
Connecticut privacy policy requirement § 42-471
Nebraska requirement related to statements in privacy policies § 87-302(14)
Pennsylvania requirement related to statements in privacy policies 18 Pa. C.S.A. § 4107(a)(10)

The fifty states have a variety of privacy and confidentiality/data protection laws dealing with:

(1) patient access to their medical records;
(2) restrictions on disclosure of identifiable medical records;
(3) rules relating to confidentiality-privilege of records documenting communications between patients and health care professionals including mental health professionals; and
(4) condition-specific laws which target certain medical conditions.

Each category of law has its state specific remedies, penalties, and fines.

(1) Access. States vary in whether or not they have specific statutes granting patients the right to access their medical records. For example, Arizona requires health care providers to allow access by patients to their medical records with limited reasons to deny such access such as protecting the health, safety or medical information of another person [Ariz. Rev. Stat. § 12-2293]. Some states may have no specific laws regarding patient access to their medical records.

(2) Disclosure. Restrictions on disclosure of identifiable medical records may target various entities such as, but not limited to, Health Maintenance Organizations (HMOs) [Neb. Rev. Stat. §§ 44-32,172, 44-7210], Managed Care Entities [Idaho Code § 41-3930(d)], Pharmacists [Idaho Code § 54-1727], Physicians [Idaho Code § 54-1814(13)], Physician Assistants [Ariz. Rev. Stat. §§ 12-2292, 12-2291], State Government [Idaho Code § 9-

45 The National Council of State Legislatures (NCSL) maintains a website that provides information on state privacy and data breach notification requirements at http://www.ncsl.org/default.aspx?TabID=756&tabs=951,71,539#951.

340C(13)], and Utilization Review Agents [Ala. Code § 27-3A-5(a)(7)], etc. Usually a patient's written consent is required to disclose their information unless another state law requires disclosure of the information.

(3) Privilege-confidentiality. Some states recognize a number of health care provider-patient privileges that allow patients, in legal proceedings, to refuse to disclose and to prevent others from disclosing confidential communications made with a professional for the purpose of diagnosis and treatment. Some statutes from Arizona are: [Ariz. Rev. Stat. §§ 12-2235 (physician or surgeon-patient); 13-4430 (crime victim counselor-victim); 32-2085 (psychologist-patient); and 32-3283 (behavioral health professional-client)].

(4) Condition-specific. Some states have registries for patients for specific conditions such as cancer [Ala. Code §§ 22-13-33; 22-13-34; 36-12-40], and birth defects [Alaska Administrative Code 7 AAC 27.012; Delaware Administrative code Title 16 § 4101] where the identifying information is confidential, privileged and not open to the public [Alaska Administrative Code 7 AAC 27.890]. Other states require reporting of communicable diseases and HIV/AIDS [Ind. Code Ann. § 16-41-2-1], but protect individually identifiable health information while allowing release with an individual's consent, to enforce public health laws or to protect the life of a named party [Ind. Code Ann. § 16-41-8-1(b)]. For mental health conditions some states require mental health practitioners to obtain a patient's written consent to disclose confidential communications about the patient including facts about the patient's treatment, although disclosure without consent is allowed in circumstances where the patient presents a danger to others or himself [Mass. Gen. Laws Ch. 112 § 129A]. Other states have chronic disease surveillance systems [Ariz. Rev. Stat. § 36-133]. Genetics testing is another condition that is regulated by states by not allowing the results to be used to discriminate, such as for insurance decisions [Ala. Code §§ 27-53-1, 27-53-2]. Information pertaining to sexually transmitted diseases is prohibited from disclosure by some states unless it is required to prevent the spread of disease [Ala. Code §§ 22-11A-14, 22-11A-22 and 22-11A-38].

For a complete in-depth report on state health privacy laws please see "The State of Health Privacy," a two-volume survey of state privacy statutes.[46/]

The Obama Administration's recent White Paper specifically recognizes the importance of state-level Attorneys General as a resource in the area of privacy enforcement and has called upon the U.S. Congress to enact legislation that would give authority to both the FTC and state Attorneys General to enforce the Consumer Privacy Bill of Rights.[47/]

C. Does your country have constitutional provisions that address or implicate privacy/data protection, such as, for example, specific data protection provisions, freedom of expression provisions or habeas data? If so, please describe these provisions and attach copies of the relevant texts.

Freedom from arbitrary and unlawful interference with privacy is protected under the Fourth Amendment to the U.S. Constitution. The Fourth Amendment, with certain exceptions, prohibits the government from conducting unreasonable searches and seizures. Government searches and seizures

46 Available at http://hpi.georgetown.edu/privacy/publications.html.
47 White Paper, at pp. 37-38.

are presumptively unreasonable if conducted without a warrant, unless one of the established exceptions to the warrant requirement applies; all warrants must be based on probable cause to believe that a crime has been, will be, or is being committed.

The Fourth Amendment to the U.S. Constitution generally does not govern privacy infringements by commercial actors. Several U.S. state constitutions contain references to privacy that may be interpreted differently by their respective judicial bodies.[48/]

D. Does your country include self-regulatory codes of conduct or similar accountability systems for privacy/data protection? If so, please describe these systems briefly and attach copies of any relevant provisions and documents which describe their operation.

Yes, many self-regulatory codes of conduct for privacy exist in the United States. Generally, the FTC has viewed industry self-regulation as a viable regulatory tool in numerous areas. Reasons for this favorable view of self-regulation include (i) the relative speed and flexibility with which such rules can be developed or adapted to changing circumstances (compared to laws) and (ii) the fact that industry representatives may have the necessary specialized knowledge for developing appropriate standards for a given industry. It is important to note that the term "self-regulation" does not imply a lack of enforceability and oversight. When businesses publicly represent that they adhere to any self-regulatory code of conduct, their compliance with such codes becomes enforceable under the FTC Act, which prohibits unfair and deceptive business practices. The failure to comply with such codes of conduct would be treated as a misrepresentation to consumers. Thus, "self-regulation" in this context may also be described as "co-regulation."

Industry initiatives include examples such as the Codes of Conduct for the Mobile Marketing Association[49/] and the Interactive Advertising Bureau.[50/] The Digital Advertising Alliance, an industry coalition of media and marketing associations, has adopted a set of Self-Regulatory Principles for Online Behavioral Advertising and an improved disclosure and consumer choice mechanism offered through a behavioral advertising icon. Three of the major browser vendors—Mozilla, Microsoft, and Apple—recently announced the development of new choice mechanisms for online behavioral advertising that seek to provide increased transparency, greater consumer control and improved ease of use. Recently, Mozilla also introduced a version of its browser that enables Do Not Track for mobile web browsing. The DAA also has established an enforcement program managed by the Better Business Bureau. On February 22, 2010, the DAA announced that that it will immediately begin work to add browser-based header signals to the set of tools by which consumers can express their preferences under the DAA Principles.[51/] Key stakeholders have also come together

---

48 See National Conference of State Legislatures listing at http://www.ncsl.org/issues-research/telecommunications-information-technology/privacy-protections-in-state-constitutions.aspx.
49 See http://mmaglobal.com/policies/code-of-conduct.
50See http://www.iab.net/public_policy/codeofconduct.
51 DAA Press Release, Feb. 22, 2012, available at http://www.aboutads.info/resource/download/DAA_Commitment.pdf. See also "White House Unveils 'One-Click' Privacy Plan," Bangkok Post, Feb. 23, 2012, available at http://www.bangkokpost.com/tech/computer/281239/white-house-unveils-one-click-privacy-plan; "No me sigas," El Pais, Feb. 23, 2012, available at http://tecnologia.elpais.com/tecnologia/2012/02/23/actualidad/1329984921_916013.html.

in a World Wide Web Consortium working group to develop standards for Do Not Track mechanisms.

TRUSTe, a private sector trustmark organization, has a privacy seal program that certifies web sites' privacy policies, monitors them and provides for complaint resolution. Violation of the TRUSTe Program Requirements may result in termination (including revocation of privacy seal) and/or referral by TRUSTe to appropriate government authorities. Also, the Better Business Bureau's online seal for businesses, includes privacy and data security requirements.

The Children's Online Privacy Protection Act and its implementing regulations (the COPPA Rule), *see above*, provide for FTC-approved, self-regulatory safe harbor programs tracking the COPPA rule requirements. There are currently four COPPA safe harbor programs. These programs have primary responsibility for ensuring their members' compliance with their requirements but a subject to enforcement by the FTC. The Safe Harbor Rule is currently under review for an update.

In addition to these codes of conduct, the U.S. government has participated in the development of codes of conduct designed to increase international interoperability between various privacy regimes. The U.S.-EU Safe Harbor Framework[52/] is a successful early example of a cross-border privacy code of conduct. The Safe Harbor was developed by the U.S. Department of Commerce in consultation with the European Commission to provide a streamlined means for U.S. organizations to comply with the European Commission's Directive on Data Protection. The U.S.-EU Safe Harbor was approved in 2000 and a similar agreement, the U.S.-Swiss Safe Harbor Framework, was finalized in 2009. The Safe Harbor Frameworks have helped bridge the differences between the European and U.S. approaches to data protection and have permitted thousands of companies to transfer data from Europe to the United States in support of transatlantic trade. As with most codes of conduct, the decision by U.S. organizations to enter the Safe Harbor program is entirely voluntary. Organizations that decide to participate in the Safe Harbor program must comply with the Frameworks' requirements and self-certify their compliance annually to the Department of Commerce. The Frameworks include principles of notice, choice, onward transfer, access, security, data integrity and enforcement. As part of their Safe Harbor program obligations, organizations are required to have in place procedures for verifying compliance with their commitments and an independent dispute resolution system to investigate and resolve individual complaints and disputes. Organizations' commitments to comply with the Safe Harbor Frameworks are enforceable by either the Federal Trade Commission or the Department of Transportation with respect to air carriers and ticket agents.

On November 13, 2011, President Obama and representatives from the other APEC economies endorsed the APEC Cross-Border Privacy Rules at a meeting in Honolulu, Hawaii. The APEC privacy system is a self-regulatory code of conduct designed to create more consistent privacy protections for consumers when their data moves between countries with different privacy regimes in the APEC region. Companies that wish to participate in the APEC privacy system will undergo a review and certification process by third parties "accountability agents" that will examine corporate privacy policies and practices and enforce the new privacy rules. Privacy authorities in the APEC region that choose to participate in the program will serve as backstop enforcers of the APEC privacy rules.

---

52 Documents online at http://export.gov/safeharbor/.

As stated in our response to Question I.A., the Obama Administration in its White Paper has called for Congress to pass legislation that would supplement the existing U.S. privacy framework. Additionally, in order to meet privacy challenges posed by the rapid evolution of technological innovations, the Obama Administration would like to draw on the expertise and knowledge of the private sector, and consult existing best practices, in order to create voluntary codes of conduct that promote informed consent and safeguard personal information. The codes would be developed through multistakeholder processes, in which commercial and non-commercial actors participate voluntarily. Businesses ultimately will choose whether to adopt a given code of conduct. American businesses know, however, that once they commit to a code of conduct, their obligations for handling personal data become enforceable under law by the Federal Trade Commission (FTC).

II. REGULATION/ENFORCEMENT

A. What is/are the enforcement mechanism(s) for the above privacy/data protection laws, regulations or procedures and what are the available remedies? Please describe any existing mechanism(s), and attach copies of relevant texts or documentation.

FTC Act. For violations of Section 5 of the FTC Act prohibiting unfair and deceptive business practices, the FTC may obtain injunctive relief, monetary remedies in the form of consumer redress and disgorgement of ill-gotten gains, and other appropriate equitable relief.

FCRA. 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 pre-tenses. 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).

GLB Act. The GLB Act provides for administrative enforcement by federal and state authorities. In general, the Bureau of Consumer Financial Protection is authorized to enforce the privacy provisions (but not the data security provisions) of the GLB Act with respect to a person that is subject to that Act, except for a person regulated by the Commodity Futures Trading Commission, the Securities and Exchange Commission, or by a state insurance regulator. In addition, the Federal Trade Commission is authorized to enforce the GLB Act with respect to any person that is subject to that Act, except a person regulated by a federal functional regulator or by a state insurance regulator. The GLB Act allows each of the authorized federal or agencies to seek remedies or impose penalties for violations of that Act, and type of remedy or the amount of a penalty varies depending on the specific authority granted to the federal or state agency. 15 U.S.C. § 6805.

COPPA. The COPPA deems violations to be unfair or deceptive business practices and its mandates are enforceable by the FTC, other federal regulators against entities within their specific jurisdictions, and State authorities. Violations carry civil monetary penalties.

The Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"). The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101-6108. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices. The FTC is authorized to initiate

federal district court proceedings to enjoin violations of the FTC Act and the TSR, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 57b, 6102(c), and 6105(b). When a lawsuit seeks civil penalties for violations of the TSR, the Department of Justice typically prosecutes the case on behalf of the FTC.

CAN-SPAM. The FCC and FTC share responsibility for these provisions. The FCC can enforce the FTC's restrictions on any commercial email message sent to a non-wireless device, such as a desktop computer, if:

- the sender is a communications company (telephone, radio, paging, cable, or television company), or;
- the message advertises or promotes a product or service of a communications company.[53/]

The FCC also has its own rules and enforcement authority under the CAN-SPAM Act regarding "mobile service commercial messages," which are commercial electronic mail messages that are transmitted directly to a wireless device. Among other things, such messages may not be initiated without the recipient's express prior authorization, and senders of such messages must cease sending further messages within 10 days if requested by the recipient.[54/]

The CAN-SPAM Act is intended to preempt – or replace – state anti-spam laws, but states are allowed to enforce the parts of the CAN-SPAM Act restricting non-wireless SPAM. Also, state laws prohibiting fraudulent or deceptive acts and computer crimes remain in effect.

HIPAA. HIPAA, as strengthened by the HITECH Act, provides HHS with authority to impose civil money penalties for violations of the Rules according to increasing tiers of penalty amounts for violations that are based on increasing levels of culpability. These amounts range from $100 to $50,000 or more per violation, with a calendar year cap for identical violations of $1.5 million. HIPAA also provides the Department of Justice with the authority to enforce criminal violations of HIPAA. In addition, the HITECH Act gave State Attorneys General authority to enforce the HIPAA protections by bringing civil actions on behalf of State residents for violations of the HIPAA Rules. The State Attorneys General are authorized to seek injunctive relief or damages in the amount of up to $100 per violation, with a calendar year limit of $25,000 for identical violations.

Federal Policy for the Protection of Human Subjects (Common Rule). Section 289 of the Public Health Service Act authorizes the Office for Human Research Protections (OHRP) to, on behalf of HHS, establish a compliance oversight process regarding violations of the rights of human subjects of research conducted or supported by HHS. Pursuant to this authority, OHRP may receive reports of such violations and take appropriate action.

ADA. The ADA can be enforced by the EEOC, which has created administrative remedies, the Attorney General of the United States in federal court, or by any person alleging discrimination on the basis of disability, in the same manner as Title VII of the Civil Rights Act of 1964.[55/]

---

53 See FCC website at http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email.
54 *See* 47 C.F.R. § 64.3100.
55 Section 12117 (ADA section 107).

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, 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. A person whose privacy rights were violated by a cable or satellite operator may file a complaint with the FCC or seek damages in federal court. 47 U.S.C. §§ 338(i)(7), 551(f). A person who receives an unwanted telephone solicitation, an unsolicited fax, or an unwanted commercial email message to a wireless account also may file a complaint with the FCC or seek damages in federal court. 47 U.S.C. § 227. A person who violates the prohibition in the Communications Act against unauthorized interception and publication of communications made by wire or radio is subject to possible fines or imprisonment. 47 U.S.C. § 605(e).

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. Any person who willfully and knowingly violates a regulation made pursuant to the Communications Act may be fined. 47 U.S.C. § 502. Finally, any person who willfully or repeatedly fails to comply with any provisions of the Communications Act or any regulation issued by the FCC thereunder may be subject to a monetary forfeiture penalty in a proceeding conducted by the FCC. 47 U.S.C. § 503.

FERPA is section 444 of the General Education Provisions Act (GEPA), which is commonly referred to as the Family Educational Rights and Privacy Act (FERPA).[56/] It is administered by the Family Policy Compliance Office (FPCO) in the U.S. Department of Education. [57/] The FCPO investigates alleged violations of the statutes and regulations, and provides educational agencies and institutions with technical assistance on how to comply with FERPA. In GEPA, Congress provided the Secretary with the authority and discretion to take enforcement actions against any recipient of funds under any program administered by the Secretary for failures to comply substantially with any requirement of applicable law, including FERPA.[58/] GEPA's enforcement methods expressly permit the Secretary to issue a complaint to compel compliance through a cease and desist order, to recover funds improperly spent, to withhold further payments, to enter into a compliance agreement, or to "take any other action authorized by law," including suing for enforcement of FERPA's requirements.[59/] The Secretary may use one or a combination of these enforcement tools as is appropriate given the circumstances. Additionally, the Department has the authority to impose the five-year rule against any entity that FPCO determines has violated FERPA either through an improper re-disclosure of personally identifiable information from education records or through its failure to destroy personally identifiable information from education records under the studies exception.

The PPRA is section 445 of the General Education Provisions Act (GEPA), commonly referred to as the Protection of Pupil Rights Amendment (PPRA).[60/] It is also administered by the Family Policy Compliance Office (FPCO) in the Department of Education. PPRA does not provide for a private

---

56 20 U.S.C. § 1232g; 34 CFR part 99.
57 *See* U.S. Department of Education website at http://www2.ed.gov/policy/gen/guid/fpco/index.html.
58 20 U.S.C. § 1234c(a).
59 20 U.S.C. 1234a, 1234c(a), 1234d; 1234e; 1234f; 34 CFR 99.67(a); see also United States v. Miami Univ., 294 F.3d 797 (6th Cir. 2002) (affirming the district court's decision that the United States may bring suit to enforce FERPA).
60 20 U.S.C. § 1232h; 34 CFR part 98.

right of action, but the same GEPA enforcement provisions that apply to the Family Educational Rights and Privacy Act (FERPA) generally apply to PPRA violations.

Data is not readily available on all of the state-level statutes containing privacy protections.

B. Does your country's domestic legal system provide individuals with recourse in the national court system for harm caused by privacy/data protection violations? Does it provide government authorities with the authority to enforce relevant privacy/data protection laws and regulations? If so, please describe and attach copies of relevant texts or documentation.

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 Act is enforced by federal and state authorities as well as private litigants. It allows courts to impose penalties of up to $3500 per knowing violation in actions brought by the FTC. 15 U.S.C. § 1681s(a).

ECPA imposes civil liability. Courts may award damages, attorneys' fees and costs.

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, but may not pursue both remedies, 47 U.S.C. § 207. A person whose privacy rights were violated by a cable or satellite operator may file a complaint with the FCC or seek damages in federal court. 47 U.S.C. §§ 338(i)(7), 551(f). A person who receives an unwanted telephone solicitation, an unsolicited fax, or an unwanted commercial email message to a wireless account also may file a complaint with the FCC or seek damages in state or federal court.[61/] In addition, as noted above, the FCC can take direct enforcement action against violators of the Communications Act or the regulations promulgated thereunder and may impose a monetary forfeiture penalty. *See* 47 U.S.C. § 503.

Under the Telephone Consumer Protection Act (TCPA), a person or entity may, in an appropriate State court if permitted by the laws or rules of court of that State, bring an action against a violator of the TCPA to enjoin such violations and/or recover damages.[62/]

Neither FERPA nor the PPRA provide for a private right of action.[63/]

The DPPA provides for criminal fines and civil penalties. It is enforced by federal authorities as well as private litigants.[64/]

Judicial remedies for state-level causes of action for privacy torts are generally available but can vary between states. [65/]

---

61 *See* 47 U.S.C. §§ 227(b)(3), (c)(5).
62 *See* 47 U.S.C. §§ 227(b)(3), (c)(5).
63 The U.S. Supreme Court ruled in *Gonzaga University v. John Doe*, 526 U.S. 273 (2002), that students and parents may not sue for damages under 42 U.S.C. § 1983 to enforce provisions of FERPA.
64 18 U.S.C. §§ 2723, 2724.
65 See generally Privacilla, How U.S. State Law Quietly Leads the Way in Privacy Protection, July 2002, at http://www.privacilla.org/releases/Torts_Report.pdf.

Data is not readily available on all of the other federal and state statutory privacy protections that may contain provisions for judicial redress.

C. Who are the government authorities in your country primarily responsible for enforcing privacy/data protection laws and regulations? Please describe its relation to (or independence from) the government, describe its size in terms of staff and budget and attach copies of relevant texts or documentation.

Federal Trade Commission

The FTC has both consumer protection and competition authority. It is also the U.S. primary privacy enforcement authority. FTC's privacy and data security authority is part of the agency's consumer protection mission.

It is an independent U.S. government agency headed by five commissioners who are nominated by the U.S. President and confirmed by the U.S. Senate. The President chooses one of the Commissioners to be Chairman. No more than three Commissioners can be of the same political party. Because Commissioners are nominated for staggered 7-year terms, Commissioners appointed by one President will often continue serving under the subsequent President, regardless of such subsequent President's political party.

The agency has approximately 1,100 full-time equivalent employees. Of those employees, about 50 attorneys, investigators and technologists dedicate all or much of their time to the FTC's privacy enforcement mission.

The FTC's total budget authority for FY 2011 was $292 million.

Federal Communications Commission

The FCC protects the privacy and security of consumer information collected by communications providers in the operation of their networks by enforcing and monitoring the privacy and security provisions of the Communications Act of 1934, as amended. The FCC is an independent U.S. government agency and is directed by five commissioners who are appointed by the President of the United States and confirmed by the U.S. Senate. The President selects one of the commissioners to serve as chairman. Only three commissioners can be of the same political party at any given time and none can have a financial interest in any commission-related business. All commissioners, including the chairman, have five-year terms, except when filling an unexpired term. The FCC has approximately 1,900 full-time equivalent employees.

Department of Health and Human Services

The HHS Office for Civil Rights is responsible for civil enforcement of the HIPAA Privacy, Security, and Breach Notification Rules. The Office for Civil Rights has approximately 239 staff who administer and enforce these rules and federal civil rights laws. OCR's budget was $41 million in FY 2011.

U.S. Department of Education

The FCPO at the U.S. Department of Education includes approximately 10 full-time staff.

Data is not readily available for other federal or state enforcement authorities.

D. What volume of complaints relating to privacy/data protection violations do your relevant government authorities receive? Do your authorities address each individual complaint or do they have discretion in which matters to investigate or pursue?

Federal Trade Commission: In 2011, the FTC received more than 1.8 million consumer complaints relating to its consumer protection mission. A portion of these complaints relate to the FTC's privacy and data security enforcement mission. The FTC does not address each individual complaint. Instead, the FTC exercises its prosecutorial discretion in selecting enforcement matters. *See* answers on case selection criteria in E below.

HHS HIPAA complaints: From April 2003 (the compliance date) to the end of 2011, HHS has received over 67,000 privacy and security complaints from individuals and others. Of those, more than 23,000 have been eligible for investigation.

OHRP. OHRP receives approximately one complaint per year related to alleged non-compliance with the HHS regulations for the protection of human subjects that pertains to privacy or data protection violations. If OHRP has jurisdiction to evaluate the possible noncompliance, the office has discretion to determine whether to conduct a compliance oversight evaluation.

FERPA. The FCPO at the U.S. Department of Education received approximately 700 pieces of written correspondence within the last calendar year, containing both complaints and requests for technical assistance.

Data is not readily available for other federal or state authorities.

E. Are the investigations and privacy/data protection enforcement actions undertaken by your authorities exclusively complaint-driven or do these authorities have other bases or criteria for selecting and initiating an investigation or enforcement action (ie. proactive audits or filing requirements)? Please explain.

Federal Trade Commission: The FTC's decisions to undertake particular privacy enforcement investigations are based on a number of factors and the existence of consumer complaints are one of these factors. Other factors include the agency's own internal research; referrals from other organizations such as relevant private sector and civil society organizations, trustmark companies and privacy advocacy organizations; media reports on new or widespread privacy problems; policy priorities as determined by the agency; the potential injury to consumers of a particular practice; the need to test and apply a new privacy law or regulation, and other relevant considerations.

Federal Communications Commission: The FCC's decisions to undertake enforcement investigations are based on a number of factors including the existence of consumer complaints, the agency's internal research concerning the relevant facts and law, media reports on new or widespread problems in the communications sector, policy priorities as determined by the agency, and the potential injury to consumers from a particular practice.

HHS (HIPAA): HHS conducts investigations both in response to complaints received as well as through event or incident driven compliance reviews. In addition, HHS has initiated an audit program to assess covered entity compliance with the HIPAA Rules.

OHRP (FERPA): OHRP conducts both for-cause compliance oversight evaluations, as well as not-for-cause compliance oversight evaluations, which can include but are not limited to concerns about the privacy of research subjects or the confidentiality of research information. For-cause evaluations occur, at OHRP's discretion, in response to OHRP's receipt of substantive written allegations or indications of non-compliance with the HHS regulations. Not-for-cause compliance oversight evaluations are conducted in the absence of substantive allegations or indications of noncompliance. Institutions are selected for not-for-cause evaluation based on a range of considerations, including: (a) the volume of HHS-conducted or -supported research in which they are engaged; (b) whether they have a history of a relatively low level of reporting to OHRP under the requirements of HHS regulations at 45 CFR 46.103(b)(5); (c) the need to evaluate implementation of corrective actions following a previous for-cause compliance oversight evaluation; (d) geographic location; (e) status of accreditation by professionally recognized human subject protection program accreditation groups; and (f) status of recent human subject protection evaluations or audits by other regulatory agencies (such as the Food and Drug Administration) or recent participation in quality improvement programs (such as OHRP's Quality Improvement program).

F. Are complaints relating to commercial data privacy issues subject to potential criminal prosecution? If so, explain the relationship, if any, between privacy regulators and public prosecutors in such cases and the general volume and nature of criminal proceedings.

FCRA provides for criminal sanctions for obtaining consumer report information under false pretenses.[66/]

ECPA: certain violations may carry criminal liability.[67/]

Under the Communications Act, any person who willfully and knowingly violates a provision of the Communications Act may be both fined and sentenced to imprisonment.[68/]

HIPAA: The U.S. Department of Justice (DOJ) has the authority to enforce criminal violations of HIPAA. HHS refers to DOJ those complaints implicating the criminal provisions of HIPAA. As of the end of 2011, HHS had referred 499 potential criminal violations to DOJ. HHS may not impose a civil money penalty for a violation of the HIPAA Rules that has been punished criminally.

66 15 U.S.C. § 1681q.

67 18 U.S.C. § 2511(4). *See also* 18 U.S.C. § 3121(d) (criminal penalties for Pen/Trap statute violations).

68 47 U.S.C. § 501.

III. CASE LAW

A. What is the role of case law in the protection of individuals' privacy in your country? Please attach any high court or appellate cases in your country.

U.S. judges and legal scholars have linked the privacy protections provided by the Fourth Amendment to the U.S. Constitution to the protection of physical objects and spaces from government searches to a broader sense of respect for security and dignity that are indispensible both to well-being and to participation in a democratic society.[69/] Courts have also recognized that individuals have substantive privacy interests against private parties.[70/]

The common law—particularly state level tort law—has also played a versatile role in the development of the U.S. commercial data privacy framework.[71/] The fountainhead for this development is Samuel Warren and Louis Brandeis's article *The Right to Privacy*, published in 1890. Warren and Brandeis specifically emphasized the right to keep personal information outside of the public domain. Their work laid the foundation for the common law development of privacy, understood by some as a broader "right to be let alone," including a right to control personal information, during much of the 20th Century.[72/]

IV. CROSS-BORDER COOPERATION

A. Does your country's domestic legal system limit or condition the transfer of any personal data to other countries? If so, please explain.

Under U.S. law, there are no general restrictions on cross-border data transfers. However, cross-border transfers of medical and health-related data by private sector organizations regulated by HIPAA need to comply with the HIPAA Rules – e.g., be for a permissible purpose and subject to reasonable and appropriate safeguards. Further, information and evidence sharing, including personal data, between U.S. enforcement authorities and their foreign counterpart authorities is subject to

---

69 *See, e.g.*, *City of Ontario v. Quon*, 130 S.Ct. 2619, 2627 (2010) ("The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government.") (citations omitted); *Kyllo v. United States*, 533 U.S. 27, 31 ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (internal quotation and citation omitted); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("They [the Framers] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men.").

70 *See Mainstream Marketing Services., Inc. v. FTC*, 358 F.3d 1228, 1232-33 (10th Cir. 2004) (holding that advancing consumer privacy is an important government interest and that restricting commercial telemarketing calls protects this interest and does not violate the First Amendment).

71 *See generally* Privacilla, How U.S. State Law Quietly Leads the Way in Privacy Protection, July 2002, at http://www.privacilla.org/releases/Torts_Report.pdf.

72 Not all courts and scholars have viewed privacy as a broad "right to be let alone." Dean William Prosser examined common law privacy cases and argued that the common law right of privacy is confined to four tort causes of action: intrusion upon seclusion, public disclosure of private facts, putting an individual in a false light, and appropriation of an individual's name or likeness. *See* William L. Prosser, Privacy, 48 CALIFORNIA LAW REVIEW 383, 389 (1960).

confidentiality requirements found in applicable laws, regulations, mutual legal assistance treaties (MLATs) and other cooperation agreements.

B. Has your country received a privacy/data protection certification by the European Union?

Yes, the United States has negotiated with the European Commission the U.S./E.U. Safe Harbor Framework that satisfies the E.U.'s "adequacy" requirement of the European Data Privacy Directive. Companies that join this program may legally transfer personal data from the E.U. to the U.S. in accordance with the Safe Harbor Framework's privacy principles.

C. Is your country a party to any international instruments or arrangements regarding general privacy principles and the cross-border flow of information (e.g., the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; the APEC Privacy Guidelines and Cross Border Privacy Rules; the Council of Europe's Convention ETS No. 108). If so, please list these instruments or arrangements to which your country is a party, the date on which they became enforceable in your jurisdiction and what actions have your country has taken, if any, pursuant thereto.

The United States has helped develop as well as endorsed both the OECD Privacy Guidelines and the APEC Privacy Framework. Further, the United States has helped develop the APEC Cross-Border Privacy Rules and intends to participate in that program once it becomes operational. The APEC Cross-Border Privacy Rules are a self-regulatory program with government backstop enforcement. Thus, once it is operational and U.S. companies subject to FTC jurisdiction join the program, the FTC will be able to enforce the APEC Cross-Border Privacy Rules against such companies.

D. Do the laws in your country permit the relevant enforcement authorities to share investigation and enforcement information and evidence with their counterpart authority in foreign jurisdictions? If so, please explain.

Yes. The FTC has a long track record of cross-border cooperation and information sharing, including in privacy-related cases. In 2006, the U.S. SAFE WEB Act further enhanced the FTC's ability to engage in cross-border cooperation. Among other things, it gives the FTC the authority to provide evidence to foreign law enforcement agencies to support appropriate foreign investigations or enforcement actions.

Foreign law enforcement agencies may submit a request for information sharing or investigative assistance under the U.S. SAFE WEB Act. A foreign law enforcement agency is defined by statute as any agency or judicial authority of a foreign government (including a foreign state, its political subdivision, or a multinational organization comprised of foreign states) that has civil, criminal, or administrative law enforcement or investigative authority. It also includes any multinational organization acting on behalf of such an entity.

The foreign agency must provide a written certification that the materials provided will be maintained in confidence and will be used only for official law enforcement purposes. The foreign agency must also identify the legal basis for its authority to maintain the material in confidence.

The FTC may share compelled or confidential information with foreign law enforcement agencies if the materials will be used to investigate or pursue enforcement proceedings related to possible violations of:

- foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by laws the Commission administers;
- a law the Commission administers, if disclosure of the material would further a Commission investigation or enforcement proceeding; or
- with approval of the U.S. Attorney General, other foreign criminal laws, if they are offenses defined in a criminal mutual legal assistance treaty between the U.S. and the requesting country.

The above criteria also apply to privacy-related violations. If the matter relates to a bank, savings and loan institution, or credit union, the FTC must obtain prior approval from the relevant regulators before sharing the information.

E. Does your government or its enforcement authorities cooperate with other governments or counterpart authorities on investigations and enforcement matters relating to privacy/data protection, for example to address the fraudulent use, transfer or mishandling of personal data?

Yes. Under the U.S. SAFE WEB Act, the FTC may provide assistance in investigations or enforcement proceedings for violations of laws prohibiting fraudulent or deceptive practices, or practices substantially similar to those prohibited by laws the FTC administers, including appropriate privacy violations. The U.S. SAFE WEB Act's investigative assistance authority excludes foreign investigations or actions in which the targets are banks, savings and loan institutions, federal credit unions, and common carriers, which are not within the FTC's jurisdiction.

The principal type of investigative assistance the FTC may provide is issuing an administrative subpoena to compel documents or other evidence. The FTC has obtained information on behalf of foreign enforcement authorities from several companies, including domain name registrars, email service providers, and telephone service providers, using this mechanism. In so doing, the FTC has successfully provided subscriber information to foreign agencies that has helped them to confirm the identity of suspects operating foreign scams, as well as identify additional victims of those scams. The Act also authorizes the FTC to use other mechanisms for obtaining information on behalf of foreign agencies.

When deciding whether to provide investigative assistance, the FTC must consider the following factors:

- whether the requesting foreign law enforcement agency has agreed to provide or will provide reciprocal assistance (not necessarily in the same matter);
- whether approval of the request would prejudice U.S. public interest; and
- whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons.

F. If cross-border collaboration exists, is this collaboration informal, does it take place via privacy/data protection regulators, or does it take place via cross-border cooperation networks (i.e. Global Privacy Enforcement Network (GPEN), APEC's Cross Border Privacy Enforcement Arrangement, or Iberoamerican Network of Data Protection)? If so, please describe this collaboration and/or your countries participation in said networks.

In the case of the FTC, collaboration is both informal and formal and both with members and non-members of GPEN and the APEC CPEA. The FTC believes that cooperation networks and frameworks such as GPEN and the APEC CPEA are invaluable in enhancing cross-border cooperation. Thus, the FTC has actively participated in developing both GPEN and the APEC CPEA.

G. If does not exist, could some form of cross-border collaboration among OAS member states assist with the enforcement or implementation of your country's privacy/data protection laws? If so, provide suggestions for what would be most useful.

Some collaboration among OAS member states already exists but could be strengthened through existing organizations and networks. For example, the FTC strongly encourages all privacy authorities in OAS member states that are also APEC members to participate in the APEC CPEA, and that all privacy authorities in OAS member states join the Global Privacy Enforcement Network (GPEN).

V. HABEAS DATA

A. Does your country's domestic legal system include laws providing for access to information about oneself, including habeas data? If so, please characterize what rights individuals may exercise under habeas data, describe the source of the right briefly, describe whether said right apply to the private and/or public sector contexts and attach copies of the provisions and the documents containing them.

The United States does not have a right called "habeas data"; however, the right of access to one's own files is a widely recognized component of the Fair Information Privacy Principles, or FIPPs, originally developed by the U.S. Department of Health, Education and Welfare in the early 1970s; accordingly, a right of access is contained in most if not all of the federal and state-level privacy laws described above. *See, e.g.,* section 609 of FCRA (Disclosures to Consumers).[73/]

The HIPAA Privacy Rule provides individuals with a right to access their medical records and other health records held by both public and private HIPAA entities, including health care providers, health plans and health care clearinghouses.

The discovery process that accompanies civil litigation in the United States is also an important method for gaining access to information about oneself. The U.S. Federal Rules of Civil Procedure, Rule 26, provides that "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody,

73 15 U.S.C. § 1681g, available at http://www.ftc.gov/os/statutes/031224fcra.pdf.

condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[74/]

Finally, the U.S. Freedom of Information Act and various state-level counterparts (sometimes referred to as "sunshine laws" or "open government" laws) also provide a means for individuals to access data about themselves and help to enhance transparency in government agency decision-making.[75/]

VI. TECHNOLOGY AND BUSINESS CHALLENGES

A. Are there any technologies or business practices that pose particular challenges for the enforcement or implementation of privacy/data protection laws and/or other consumer protection laws in your country? If so, describe.

Rapid developments in modern information technology and in the business practices this technology facilitates pose serious challenges for all privacy regimes. However, it may be premature to name particular technologies at this point. Technology continues to develop quickly, and the Administration believes that multistakeholder processes such as those envisioned in the White Paper can be flexible and could offer the most effective solution to the challenges posed by a rapidly changing technological, economic, and social environment. This recommendation reflects the Administration's view that government must support policy development processes that are nimble enough to respond quickly to consumer data privacy issues as they emerge and that incorporate the perspectives of all stakeholders to the greatest extent possible. A well-crafted multi-stakeholder process will allow stakeholders to address privacy issues in new technologies and business practices without the need for additional legislation, permit stakeholders to readily reexamine changing consumer expectations, and enable stakeholders to identify privacy risks early in the development of new products and services.

The fact that data flows are increasingly global in nature compounds our challenges because it requires the development of privacy regimes that not only are able to accommodate constant changes in technology and business practices but that also allow for interoperability and cooperation across different jurisdictions with different legal regimes. One recent example of an attempt to create such a flexible cross-border interoperability scheme are the APEC Cross-Border Privacy Rules, which are a negotiated, multilateral self-regulatory privacy program for businesses that is backed up by government privacy enforcement authorities.

74 FRCP Rule 26 Duty to Disclose, available at http://www.law.cornell.edu/rules/frcp/rule_26.
75 See state-level overview at http://sunshinereview.org/index.php/State_sunshine_laws.