PERMANENT COUNCIL OF THE
ORGANIZATION OF AMERICAN STATES

COMMITTEE ON POLITICAL AND JURIDICAL AFFAIRS

OEA/Ser.G
CP/CAJP-3063/12
3 April 2012
Original: English/Spanish

COMPARATIVE STUDY: DATA PROTECTION IN THE AMERICAS

Different existing legal regimes, polices and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation

[Document presented by the Department of International Law, of the Secretariat for Legal Affairs, pursuant to operative paragraph 10 of General Assembly Resolution AG/RES. 2661 (XLI-O/11)]

COMPARATIVE STUDY: DATA PROTECTION IN THE AMERICAS

Different existing legal regimes, polices and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation

-- Table of Contents --

COMPARATIVE STUDY: DATA PROTECTION IN THE AMERICAS

Different existing legal regimes, polices and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation

[Document presented by the Department of International Law, of the Secretariat for Legal Affairs, pursuant to operative paragraph 10 of General Assembly Resolution AG/RES. 2661 (XLI-O/11)]

I. INTRODUCTION

The General Assembly of the Organization of American States has long placed special attention to matters concerning access to information and privacy/data protection. As part of these efforts, resolution AG/RES. 2661 (XLI-O/11), adopted at the fourth plenary session on June 7, 2011, which, instructed the Department of International Law to present this comparative study of different existing legal regimes, polices, and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation ("comparative study"), with a view to exploring the possibility of a regional framework in the area.[1]

As follow-up to resolution AG/RES. 2661 (XLI-O/11), the Permanent Council's Committee on Juridical and Political Affairs (CJPA), at its ordinary session held on October 6, 2011, established a calendar and drafting methodology, as well as the process for OAS Member States to provide the inputs on their existing legal frameworks on privacy/data protection necessary for the study. At this session of the CJPA, State Delegations requested the drafting of a Questionnaire Regarding Privacy and Data Protection Legislation and Practices so that OAS Member States may provide the requested information in a standardized format. The Questionnaire circulated via document CP/CAJP-3026/11 on October 31, 2011. Member States agreed on a due date of January 15, 2012 (extended to February 15, 2012) for State Responses to the Chair of the Committee. It was agreed that drafting of the study would also be informed by contributions from other organs, organisms and agencies of the Inter-American System, particularly the work of the Inter-American Juridical Committee (including its study on access to information and data protection in document CP/doc. 4193/07) and inputs from other international organizations working in the field of privacy/data protection.

A total of eleven Member States replied to the questionnaire: Argentina, Canada, Colombia, Costa Rica, Dominican Republic, El Salvador, Mexico, Panama, Peru, United States and Uruguay. Information provided in these responses form the main part of the present study. Also included in the present study are brief updates on the work of international organizations, including the Asia Pacific Economic Cooperation, the Council of the Europe, the European

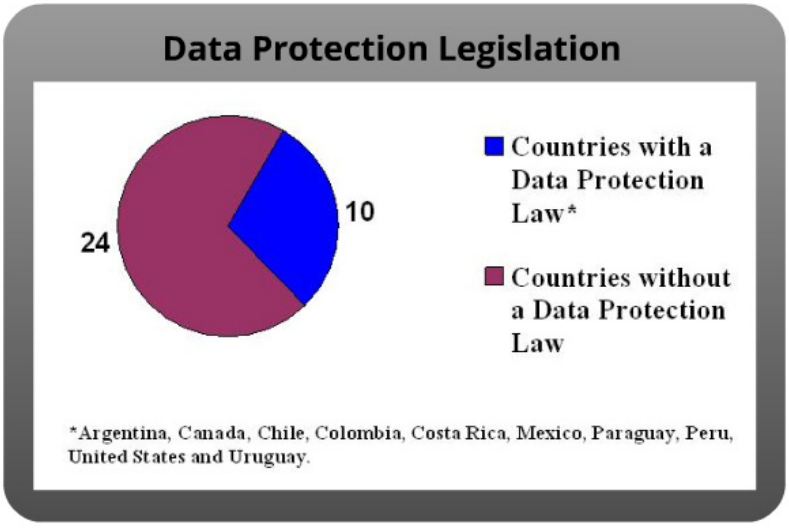
[1] AG/RES. 2661 (XLI-O/11), adopted June 7, 2011. As part of its rationale for requesting the study, the General Assembly recalled that access to public information, on the one hand, and the protection of personal data, on the other, are fundamental values that must operate in harmony at all times; considering the growing importance of privacy and the protection of personal data, and the need to encourage and protect cross-border flows of information in the Americas; bearing in mind the efforts made by states to ensure access to public information and the protection of personal data and the efforts of other international and regional bodies (such as OECD, APEC, EU, and the Council of Europe) working in the area of protection of personal data; and taking note of the Preliminary Principles and Recommendations on the Protection of Personal Data contained in document CP/CAJP-2921/10 rev. 1, prepared by the Department of International Law (DIL), and the comments offered on it by the member states,

Union, the Ibero-American Network on Data Protection, and the Organization for Economic Cooperation and Development.

Section II of the study provides a general comparative perspective on existing legal frameworks on privacy/data protection. Section III provides brief summaries of the international instruments adopted and/or work being conducted on privacy/data protection by other international organizations. Section IV describes the local legal frameworks on privacy/data protection for OAS Member States.

II. General Legal Frameworks

Legislation on data protection is based on an individual's right to privacy. However, the meaning of privacy and the origins of an individual's right to privacy can vary. As a result, policies and laws governing the right to privacy differ from country to country. Because of this divergence in the treatment of the right to privacy, legislation protecting the treatment of personal data can vary between or even within regions. Generally speaking, the treatment of data protection has followed one of three approaches. The European system is the strictest current system of government-regulations with legislation governing both the collection of personal data by the government and private organizations. The United States' follows a bifurcated approach, which allows industry regulation of personal data collected by private organizations and government regulation of data collected by the government. And finally, several Latin American countries have data protection mechanisms based on the writ of *Habeas Data*, which is a constitutional right that allows individuals to access to their own personal data and the right to correct any mistaken information. Several Latin American states have also recently adopted comprehensive legislation on privacy/data protection.



The Universal Declaration of Human Rights and the United Nations International Covenant on Civil and Political Rights, define privacy as the right to not "be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon [an individual's] honour and reputation." Both agreements go on to explain that "everyone has the right to the protection

of the law against such interference or attacks." The Council of Europe also recognizes the right to privacy as a "fundamental human right."

In most countries, the right to privacy can be traced back to the constitution. In the United States and Canada for example, privacy stems in large part from constitutional provisions against unreasonable searches and seizures. In its decisions, the Court has stated that the Constitution protects "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions."[2] However, the Court has also held that the right to privacy was not absolute and an individual's privacy interest must be balanced against "competing public interests."[3]

In Latin America, the constitutional frameworks of several countries define privacy as the right to not be subjected to arbitrary interference with a person's privacy, family, home or correspondence, and right to be free from attacks an individual's honour and reputation, following definitions found in Universal Declaration of Human Rights and the Covenant on Civil and Political Rights. Some constitutions include the right to data protection and include provisions on the writ of habeas data.

Constitutional Provisions which expressly provide for a right to Privacy, Habeas Data and/or Data Protection

Country	Privacy	Habeas Data	Data Protection
Argentina	Yes art. 18	Yes art. 43	No
Brazil	Yes art. 5	Yes art. 5	No
Canada	Yes section 7 & 8	No	No
Chile	Yes art. 19	No	No
Colombia	Yes art. 15	Yes art. 15	No
Costa Rica	Yes art. 24	No	No
Dominic Republic	Yes art. 44	Yes art. 70	Yes art. 44
Ecuador	Yes art 66	Yes art. 94	Yes art. 66
El Salvador	Yes art. 2	No	No
Guatemala	Yes art. 25	Yes art. 31	No
Mexico	Yes art. 6	Yes art. 16	Yes art. 16
Panama	Yes art. 29, 17, 37	Yes art. 44	No
Paraguay	Yes art. 30	Yes art. 135	No
Peru	Yes art. 2	Yes art. 200	Yes art. 2
United States	Yes 4th amendment	No	No
Uruguay	Yes art. 7	No	No
Venezuela	Yes art. 60	Yes art. 281	Yes art. 28

III. International Instruments on Privacy/Data Protection

[2] In the Unites States, the right to privacy has often been defined as "the right to be let alone," and the United States Supreme Court has ruled in favor of privacy interests by deriving the right to privacy from the fourth amendment to the constitution.

[3] Id.

Multilateral organizations have undertaken intensive efforts over the past decades to adopt guidelines, principles, recommendations and/or binging legal instruments, at the regional and international level, in particular within the Organization for Economic Cooperation in Europe (OECD), the Council of Europe (COE), the European Union (EU), and the Asia-Pacific Economic Cooperation (APEC) forum. There is a commonality in these instruments, which apply to and have impact in varying degrees on the legal frameworks of OAS member states, and generally require that personal information must be obtained fairly and lawfully; be used in ways that are compatible with the original specified purpose; accurate, relevant and proportional with respect to purpose; accurate and up to date; limited in distribution to others; and be destroyed after its purpose is completed. At the same, there are some significant differences in the approaches represented in these instruments as well, including whether, when and how to apply the same principles to governmental entities, public service providers, private commercial enterprises, and even individuals; issues of criminal law enforcement and national security.[4]

A. APEC

For several years the Asia-Pacific Economic Cooperation (APEC) forum has been working on a privacy initiative. Rather than pursuing harmonization of domestic privacy laws, however, this work has focused on the issue of trans-border transfers of personal data. A Framework with Privacy Principles was adopted in 2004, and an implementation program was added in 2005 to encourage domestic implementation of the Principles by individual member states. A Data Privacy Sub-group has been working to develop Cross Border Privacy Rules (CBPR) allowing businesses to be certified for transfer of personal information between participating APEC economies. A Cross Border Privacy Enforcement Cooperation Arrangement (CPEA) was established in 2010 to provide mutual recognition between participating APEC economies of each other's mechanisms for certification of a business's privacy rules. (The OECD has a similar enforcement network called GPEN.)

B. Council of Europe

The COE's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* broadly defines personal data as "any information relating to an identified or identifiable individual" and outlined data protection principles, which have served as the basis for data protection legislation worldwide.[5] The convention consists of three main parts: substantive law provisions in the form of basic principles; special rules on transborder data flows; and mechanisms for mutual assistance and consultation between the Parties.

The convention's point of departure is that certain rights of the individual may have to be protected vis-à-vis the free flow of information across border.[6] Where the present convention imposes certain restrictions or conditions on the exercise of freedom of information, it does so only to the extent strictly justified for the protection of other individual rights and freedoms, in particular the right to respect for individual privacy.[7]

---

[4] Preliminary Comments on a Statement of Principles for Privacy and Personal Data Protection in the Americas, CJI/doc.382/11.

[5] *See* Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data arts. 2, 4-12, Jan. 28, 1981.

[6] Explanatory note to Convention 108. This principle is enshrined in international and European instruments on human rights. see Article 10, European Human Rights Convention; Article 19, International Covenant on Civil and Political Rights.

[7] Article 8, European Human Rights Convention

Convention 108 is currently undergoing a revision process to pursue two main objectives: to deal with challenges for privacy resulting from the use of new information technologies and to strengthen the Convention's follow-up mechanism.

C. European Union

The European Union's *Data Protection Directive* ("Directive") acknowledged the individual's right to privacy and set a standard level of data protection for members of the European Union.[8] Because of this an expansive concern over an individual's right to privacy, the Directive goes on to allow the transfer of personal data to countries outside the European Union only if the country ensures "an adequate level of [data] protection," or if the transferor has otherwise demonstrated that the data will be adequately protected once transferred[9] In this way, the Directive extends the reach of protection afforded to personal data originating in the European Union to countries outside its borders.

The Directive's reach has extended past EU borders, influencing data protection regulation worldwide by forcing other countries with companies interested in transferring personal data to examine their own data protection legislation and, if necessary, to change their legislation to meet the European Union's standards.[10] It is important to point out, however, that the European Commission launched a review of the Directive in 2010 based in part on the recognition that "there is a general need to improve the current mechanism for international transfers of data." The Vice President of the European Commission responsible for the Digital Agenda, has also explained that the EU's data protection framework must be updated for the digital era in order to ensure fundamental rights while at the same time "deliver[ing] the better economy and better living that digital technologies make possible." A proposal for new legislation to replace the Directive is anticipated later this year

D. Organization for Economic Cooperation and Development

The Organization for Economic Cooperation and Development adopted nonbinding, technologically-neutral principles for possible use in establishing either a legal framework or an industry standard. The eight "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" apply to both governmental and commercial uses of personal data.[11] They call for (1) limiting the collection of personal data and ensuring that such information should only be obtained by lawful and fair means and, where appropriate, with the knowledge o consent of the data subject; (2) ensuring that the information collected should relevant to the purposes for which they are to be used, accurate, complete and up-to-date; (3) specifying the purposes for which personal data are collected; (4) not disclosing or using data for purposes other than those specified in advance; (5) protecting the data by reasonable security

[8] *See* Stratford, at 19 (adding that the *Directive*, which was adopted in 1995, directed member states to ensure that their national privacy laws were in compliance with its standards).
[9] Id.
[10] Id. at 19-20.
[11] Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, adopted in 1980, available at: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

safeguards; (6) establishing a general policy of openness about developments, practices and policies with respect to personal data; (7) giving individuals the right to obtain personal data within a reasonable time and in a reasonable manner; and (8) holding data controllers accountable for complying with the requirements of these principles.

OECD governments also adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.[12] Among other topics, the recommendation called for the establishment of an info rmal network of privacy enforcement authorities.[13] The Global Privacy Enforcement Network (GPEN) is an OECD effort – similar to APEC's CPEA – to give effect to the recommendation.[14]

IV. National Legal Frameworks

The discussion of privacy/data protection at the level of the Member States is divided into four sections. Section A of each describes, to the extent of the information available, whether the State constitution establishes a right to privacy, a right to data protection and/or a writ of habeas data; analyzes whether the State has enacted (comprehensive, sectoral or principle-based) legislation on privacy/data protection, or and/or legislation on habeas data; discusses whether these laws apply to private and/or public sector contexts; and, whether the local framework provides for self-regulatory codes of conduct or similar accountability systems for privacy/data protection.[15]

Section B analyzes, to the extent of the information available, whether the local system provides for and/or creates a data protection/enforcement authority and describes its relationship to (or independence from) the government; analyzes the manner in which each state enforces compliance with privacy/data protection laws, regulations and procedures; and discusses the remedies available in case of violation and describes the recourse available to individuals harmed by such violations. In cases where the information is available, it discusses the volume and types of complaints handled by or brought before the authorities, and whether such authorities have investigatory capabilities and whether violations are subject to potential criminal prosecution.

Section C describes, to the extent of the information available, each State's system for cross-border cooperation; describes whether the state places limits or conditions on transfers of personal data to other countries, discusses the framework for cross-border flows of information -- whether personal data which refers to a state resident and/or was processed in the state may be transferred to (exported to or shared with) another jurisdiction; describes the system for cross-border cooperation when a violation or breach occurs locally regarding information originating in

---

[12] Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy Adopted in 2007, available at: http://www.oecd.org/document/60/0,3343,en_2649_34255_38771516_1_1_1_1,00.html.

[13] Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, Paragraph 21 specifies a number of tasks for the network: Discuss the practical aspects of privacy law enforcement co-operation; Share best practices in addressing cross-border challenges; Work to develop shared enforcement priorities; and Support joint enforcement initiatives and awareness campaigns.

[14] The GPEN Network webpage can be found at: https://www.privacyenforcement.net.

[15] Unless a specific source or citation in this section is added by footnote, information contained herein section refers specifically to responses to the Questionnaire on Privacy and Data Protection Legislation and Practices presented by the State in question.

a foreign jurisdiction, or when a violation or breach occurs in a foreign jurisdiction regarding local personal data; describes the international agreements or arrangements to which it is party, including whether it has received privacy/data protection certification from the European Union. If the information is available, this section will attempt to discuss whether local law permits enforcement authorities to share investigation and enforcement information with authorities in foreign jurisdictions, including whether such collaboration is informal or takes place via regulators or cross-border cooperation networks (ie. Global Privacy Enforcement Network (GPEN), APEC's Cross Border Privacy Enforcement Arrangement, or Ibero-American Network on Data Protection).

Section D examines the effect of relevant case law on the privacy/date protection framework, as well as any special challenges faced by the state in question.

1. Argentina:

A. Legal Context

i. Constitutional Framework:

An analysis of constitutional rights on the topic of privacy/data protection in Argentina,[16] begins which a discussion of the relevant international instruments on the freedom of expression and information, including the American Declaration of the Rights and Duties of Man, the Universal Declaration on Human Rights,[17] the American Convention on Human Rights,[18] the International Covenant Economic Social and Cultural Rights, the International Covenant on Civil and Political Rights and its Optional Protocol.[19] These instruments have constitutional hierarchy in

[16] Constitution, arts. 14, 33 and 32.

[17] Article 19 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[18] Article 13 Freedom of thought and expression: 1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. 2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals. 3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions....

[19] Article 19: 1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Argentina,[20] and the rights enshrined in each have also been expressly included in the national constitution.[21]

With regard to privacy/data protection, Article 43 of the Constitution establishes the right of habeas data, whereby any person may file an action to obtain information on the data about him/herself, contained in public or private records/databases, and in case of false data or discrimination, a writ of habeas data may be filed to request the suppression, rectification, confidentiality or updating of said data. [22]

Article 19 incorporates the constitutional right to privacy, providing in part that the private actions of individuals, which do not offend public order, morality, or injure third parties, are reserved only to God and are exempted from the authority of judges. nor deprived of what it does not prohibit. Article 18 establishes that correspondence and private papers receive express protection, providing in part that written correspondence and private papers may not be violated.

[20] Art. 75 (22) establishes that treaties and agreements take precedence over national law.
[21] Article 14: All the inhabitants of the Nation are entitled to the following rights, in accordance with the laws that regulate their exercise, namely: to work and perform any lawful industry; to navigate and trade; to petition the authorities; to enter, remain in, ...travel through, and leave the Argentine territory; to publish their ideas through the press without previous censorship; to make use and dispose of their property; to associate for useful purposes; to profess freely their religion; to teach and to learn. Article 32: The Federal Congress shall not enact laws restricting the freedom of the press or establishing federal jurisdiction over it. Article 33: The declarations, rights and guarantees which the Constitution enumerates shall not be construed as a denial of other rights and guarantees not enumerated, but rising from the principle of sovereignty of the people and from the republican form of government.
[22] Article 43.

ii. Legislative Framework:

The Federal Argentine Law on the Protection of Personal Data,[23] and its Regulation,[24] is public order legislation applicable to the entire country, the objective of which is the protection of personal data processed by technological means. The law applies to all public databases (without limitation), as well as all private databases that are not for personal use.

The law defines and protects sensitive data, establishes the principles and requirements of data quality and processing, regulates the activities of transfer, international transfer, provision of services, credit reports and marketing activities, establishes the duty of registration of databases, measures security and confidentiality, the right of the individual (data owner) to access, rectify, correct and suppress data, creates the data protection authority, and provides administrative sanctions.[25]

ii. Habeas Data:

Law No. 25,326 on the Protection of Personal Data and its Regulatory Decree No. 1.558/2001, also regulate the judicial action of habeas data.

iv. Self Regulation:

The Data Protection Law permits the voluntary creation of "codes of conduct" whereby private associations, organizations or users of data may develop codes of conduct of professional practice, setting standards for the processing of personal data to ensure and improve the operation of information systems according to the principles set forth in the law. These codes must be entered in the register that the certification body maintains for that purpose. The authority may deny registration if it decides that the self-regulatory code does not conform to the law and regulation.[26]

To date, only one code of conduct has been registered in National Data Protection Directorate, filed and approved in 2004 by the *Asociación de Marketing Directo* under the provisions of the law.[27]

[23] Law No. 25,326.
[24] Regulatory Decree No. 1.558/2001
[25] Law No. 25,326 on the Protection of Personal Data and its Regulatory Decree No. 1.558/2001, (DNPDP Disposition No. 11/06).
[26] Law No. 25,326 article 30 and Decree 1558/2001.
[27] Resolution DNPDP No. 4/2004.

B. Enforcement

i. Enforcement Mechanism:

There are basically two (2) mechanisms to enforce the right to privacy/data protection: a) Administratively through the NDDP; and b) Judicially through a writ of Habeas Data or ordinary action.

In the administrative sphere, the NDDP receives complaints or acts on its own accord with respect to possible violations of the law.[28] Article 31 of the regulation to Law No. 25,326 applies to private and public databases. The administrative procedure is generally comprised of the following steps, initiated by the NDDP in cases of alleged violations of the provisions of Law No. 25,326 and its regulation. The NDDP may acts ex officio or upon a complaint put forward by an individual, the Ombudsman's Office, or by consumer groups or users. The NDDP will open a file in which the particular acts of the case are recorded and the alleged infraction verified. This alleged infringing party has five (5) working days present his defense in writing and provide any evidence that violations have not occurred. Upon ruling by the NDDP, appeal is permitted within 10 working days.

In the judicial sphere, the individual may initiate an action for protection pursuant to the provisions of the writ of habeas data in Article 43 of the Constitution and the data protection law: a) to get access to the personal data stored in public or private files, records or databases; and b) where the data is incorrect, false, inaccurate, outdated, etc., or when the processing is prohibited pursuant to the law, to require the rectification, suppression or update.[29]

ii. Data Protection/Enforcement Authorities:

The Argentine data protection authority is the National Directorate for Data Protection,[30] housed within the Ministry of Justice and Human Rights, but with independent exercise of its duties.[31] It has a staff of approximately 45 people and a budget from the Ministry of Justice and Human Rights.

The NDDP is required to address all complaints which may involve a violation of the law. As the supervisory body, the NDDP is authorized to receive complaints, and received an average of 500 complaints a year -- a number that has been declining as knowledge of the legal framework on privacy/data protection has been increasing.

Most complaints against private parties are for violations of the rights of access, rectification, suppression, etc. Most complaints against public sector entities are for violations of the right of access to data personal.

With regard to the volume of complaints received against private parties, approximately: 70% are against financial institutions, 10% against credit reporting companies, and 20% to utility companies and others. Of the complaints processed, the individual who brought the action prevailed in his/her claim an average of 80% of the time (access, rectification, suppression,

[28] Law 25,326 Article 31 and Decree NTA 1558/2001.
[29] Law No. 25,326, Chapter VII
[30] Law N ° 25326, Art. 29
[31] Decree No. 1558/01, Article 29

blocking, etc.). In approximately 14% it was determined that there was no of violation of existing rules. 2% of complaints were suspended because there existed parallel proceedings in the court system. In another 2% if cases the NDDP was incompetent to hear the claim and in the final 2% complaints could not be possessed due to procedural shortcomings.

iii. Administrative and Criminal Sanctions:

The law establishes administrative penalties that apply to public databases, for liability or damages arising from failure to observe the data protection law.[32] The NDDP may issue a warning, suspension, fine, closure or cancellation of the file, record or database.[33] The regulation defines the conditions and procedures for the application of the penalties, graded in relation to the severity and extent of the violation and the damages resulting from the breach. Article 31 of the regulation to Law No. 25,326 applies to private and public databases. As mentioned, penalties are set in an incrementing scale, which takes into account the nature of personal rights involved, the volume of processing operations, the benefits obtained, the degree of intent, recidivism, the damages caused to affected persons and others, and any other circumstance that is relevant to determine the degree of unlawfulness and culpability in the specific infringement. Repeat offender (those convicted of a violation of Law No. 25,326 and its regulations incur within a period of 3 years) will also receive higher penalties.[34]

The data protection law also provides for criminal penalties, which are incorporated into the National Criminal Code.[35] In general, persons who knowingly inserted false information into database may be punished with imprisonment from one month to two years. Persons who knowingly provided false information to a third party may be imprisoned by six months to three years and penalties are increased by one half the minimum and maximum, when individuals are harmed by the knowing or willful actions. When the author or responsible for the crime is a public official in exercise of his/her functions, such person is also suspended from public office for twice as long as that of the sentence. In addition the criminal code added another article to punish with imprisonment from one month to two years any individual who knowingly and unlawfully breached security systems and data confidentiality, or gained unlawful access to personal data; or disclosed information in a personal database bound to secrecy under provisions of the law. When the perpetrator is a public officer, he/she is also suspended from officer for one to four years.[36]

C. Cross-Border Cooperation

i. Data Transfer:

Argentine law prohibits the transfer of personal data to countries that do not have legislation that offers protections similar to those under Law No. 25,326. There are certain cases where this an

[32] Law No. 25,326, Art. 31. Criminal penalties may also apply pursuant to section IV below.
[33] Under the law, fines range from one thousand dollars ($ 1,000) to one hundred thousand dollars ($ 100,000).
[34] The proceeds of the fines in Article 31 of Law No. 25,326 are applied to the finances of the NDDP.
[35] Article 32 of Law No. 25,326 is incorporated by reference and later by statute into article 117 bis of the National Penal Code.
[36] 2. Article 32 of Law No. 25,326 is incorporated by reference and later by statute into article Incorporated as article 157 bis of National Penal Code.

exception to this prohibition can be obtained, for example when the individual consents to the transfer or when the importer of the data is obligated contractually to apply Law No. 25,325, provided the importer's local legislation does not prohibit the application of Argentine law.[37]

ii. International Instruments/Arrangements:

Argentina is not party to any international instruments or arrangements regarding general privacy principles and the cross-border flow of information. However, Argentina has received the adequacy certification, as a country with compatible legislation, by decision of the European Commission,[38] and participates actively in the Ibero-American Network on Data Protection.

ii. Cross-Border investigatory and enforcement cooperation:

Cross-border cooperation in Argentina generally takes place directly between the jurisdictional or administrative organs of the State on an informal and reciprocal basis. The law however does include an exception to the general prohibition against international transfer for cases of international judicial collaboration, making cross-border cooperation possible and more effective.[39]

In addition, for reasons of territorial jurisdiction, the local data protection authorities may refer cases in which violations are detected to other data protection authorities in the country or abroad. This type of cooperation has taken place in administrative proceedings, for example, arising from complaints with Spain and the UK. Locally, cooperation is performed with the consumer protection offices that exist in each province, which refer to the supervisory body all cases falling within its jurisdiction.

D. Case Law and Special Challenges

Case law in Argentina on privacy/data protection is extensive and has been instrumental in the development of this right, as well as in the implementation of the legislation. Some of the most notable cases include "Ponzetti of Balbin," "Ganora" and "Urteaga." The most recent case with nationwide impact has been the "Prudential" case.[40]

With regard to special challenges commonplace in Argentina, the Internet in general posses significant tests particularly with the regard to privacy policies governing the operation of business information services on the Internet, which require further adaptation to the protection of

---

[37] Law No. 25,326, Art. 12. Exceptions to the prohibition of international transfer apply in the following cases: a) international judicial collaboration; b) The exchange of medical data, when required by the treatment of affected or epidemiological research, it is conducted in terms of subsection e) of the preceding article; c) bank transfers or exchanges, with regard to the extent thereof, and as the legislation that is applicable; d) When the transfer is arranged within the framework of international treaties to which Argentina is a party; e) The transfer is aimed at international cooperation among intelligence agencies to combat organized crime, terrorism and drug trafficking.

[38] See the Argentina's response to Questionnaire for a copy of the EU Certification Document.

[39] Law No. 25,326, Art. 12 (a).

[40] Cases are attached to the documentation provided by Argentina as part of its response to the Questionnaire.

privacy/personal data, with special emphasis on the applicability of the right be forgotten (eg . online data that remains perpetually and interferes with the rights of individuals, even it may have no value as news. Such data frequently become historical archives of information which continue to register on Internet search engines, such as Google, Bing, etc.

Similarly, detection technologies and content localization (cellular, GPS, RFID, satellite, wireless, radar, antennas, cookies, etc.), instantly generate information on the localization and activities of individuals and requires regulation. Other technologies generate discomfort to users and require its own regulation (direct email marketing, or marketing by phone, text messaging on cell phones, etc).

2. Canada:

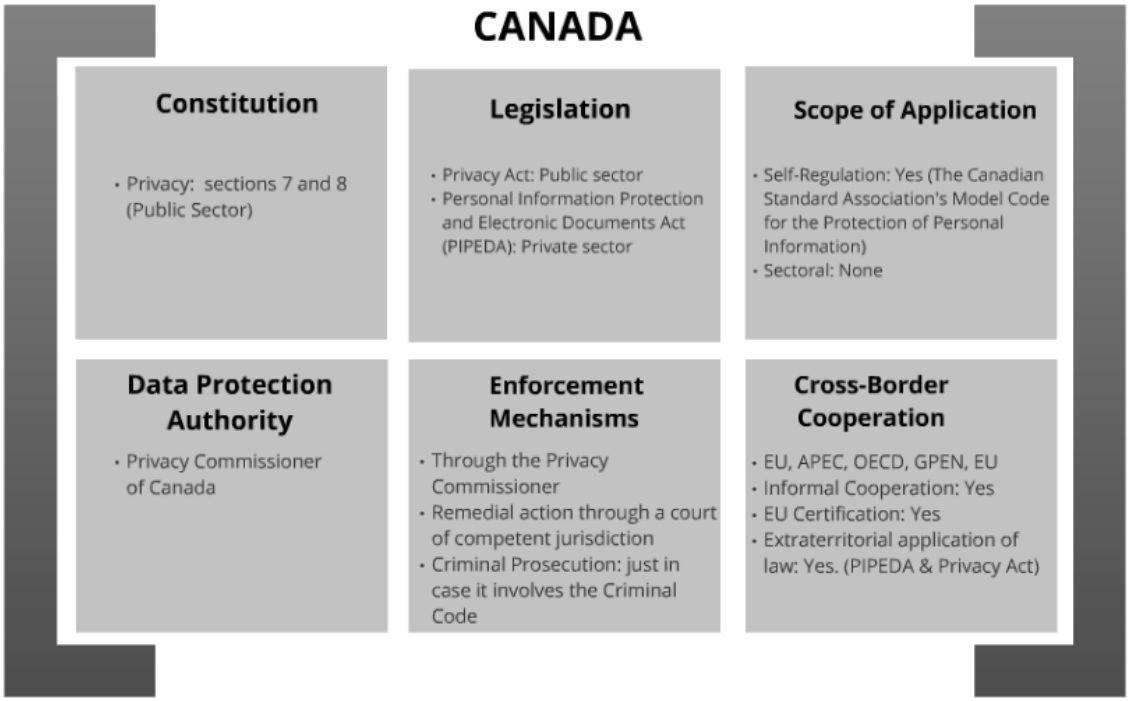
A. Legal Context

i. Constitutional Framework:

The *Canadian Charter of Rights and Freedoms* (*Charter*) forms part of Canada's Constitution and applies to all levels government: federal, provincial, territorial and municipal.[41] Every government action and decision is subject to the *Charter*. Certain actions of non-governmental entities can also be subject to the *Charter* where these essentially amount to "government actions", which is assessed according to established jurisprudential criteria.

Section 8 of the *Charter*, which reads "Everyone has the right to be secure against unreasonable search or seizure," is the main constitutional provision framing the collection, use and disclosure of personal information by government institutions and agencies. Canadian courts have interpreted section 8 broadly and contextually. Its protection encompasses a guarantee against any form of unwarranted state interference with a person's reasonable expectation of privacy. For such intrusions to be considered "reasonable", thus in compliance with s. 8, they must be authorised by law. The law itself must be reasonable and the search or seizure must be carried out in a reasonable manner. Thus, absent reasonable lawful authorisation for an intrusion, a person whose reasonable expectation of privacy has been breached – be it from any of the protected perspectives (*i.e.* physical: one's body; territorial: one's home; or informational**:** one's information disclosing intimate details of lifestyle or personal choices) – can seek a constitutional remedy, which includes damages.

[41] http://laws-lois.justice.gc.ca/eng/charter/



Section 7 of the *Charter* protects the right to life, liberty and security of the person in accordance with the principles of fundamental justice. It has, at times, been construed as also providing residual protection for privacy interests, including those pertaining to data.

While issues relating to informational privacy mainly implicate s. 8 of the *Charter*, section 2(b) can be construed as playing an ancillary role in the general protection of data. Section 2(b) constitutionally protects freedom of expression in Canada. The provision reads: "Everyone has the following fundamental freedoms: (…) (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;…" Canadian courts have interpreted this protection very generously, requiring any state-imposed restriction to satisfy the stringent justification test of section 1 of the *Charter*, which reads "The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society". The burden of the test rests with the state.

The principles underlying freedom of expression in Canada would extend to expression and data on the Internet, ensuring, for instance, a person's constitutional right to access data located on the Internet and to express themselves *via* the Internet, so long as the expression does not constitute violence or a threat thereof, or otherwise breach other applicable laws in Canada such as the *Criminal Code* prohibitions against child pornography, hate speech and incitement to terrorism. Section 2(b) includes the right to receive expression. However, absent exceptional circumstances, s. 2(b) does not formally guarantee a right of access to government information. Such a right is governed by other laws.

ii. Legislative Framework:

Federal Law: At the federal level, there are two statutes that create comprehensive privacy protection regimes: the *Privacy Act*[42] and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[43] The *Privacy Act*, which took effect in 1983, enunciates the obligations of federal government institutions regarding the collection, use, disclosure, retention and disposal of personal information. It gives individuals the right to access and request correction of personal information that Government holds about them, subject only to the exceptions in the Act. It also puts in place an independent ombudsperson, the Privacy Commissioner, to resolve problems and oversee compliance with the legislation. The *Privacy Act* also provides the right to apply to the Court for review in some limited circumstances. The *Privacy Act* must be read with the *Library and Archives of Canada Act* regarding the retention and disposal of personal information under the control of government institutions.[44]

The *Personal Information Protection and Electronic documents Act* (PIPEDA), which took effect by stages between 2001 and 2004, sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. It applies to all organizations engaged in commercial activities or that operate in a federally-regulated area of jurisdiction, such as banking, telecommunications and interprovincial and international transportation. Private sector organizations subject to provincial privacy legislation that has been recognized by Order as being substantially similar to PIPEDA are exempt from the federal Act for all intra-provincial collections, uses or disclosures of personal information. The law gives individuals control over their personal information, by requiring organizations to seek their consent prior to collecting, using or disclosing their information. Individuals also have the right to access and to request correction of their personal information held by these organizations The Act gives to the Privacy Commissioner the power to receive or initiate complaints and requires the Commissioner to investigate and report on these complaints, which may be resolved through various dispute resolution mechanisms. Unresolved matters may be taken to Federal Court, which has the power to order an organization to change its practices and award damages to the applicant.

Provincial Law: In Canada, every province and territory has privacy legislation governing the collection, use disclosure, retention and disposal of personal information held by government agencies. The provisions of these acts are not identical but all statutes are based on the same fair information principles. They regulate the powers that a government institution has to collect, use and disclose personal information and usually provide individuals with a general right to access and correct their personal information. Oversight is through either an independent commissioner or ombudsperson authorized to receive and investigate complaints.

In some provinces, the same legislation applies to the provincial and the municipal levels while in other provinces this goal is achieved by two different statutes.

Some provinces have a legislation governing the collection, use, disclosure, retention and disposal of personal information by private sector organizations that were recognized as substantially similar to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Some provinces have also passed legislation to deal only with the collection, use,

---

[42] http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html
[43] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/
[44] http://laws-lois.justice.gc.ca/eng/acts/L-7.7/

disclosure, retention and disposal of personal health information by health care providers and other health care organizations. Two of these healthcare privacy laws have been recognized as substantially similar to PIPEDA.[45]

iii. Habeas Data:

As Habeas Data is a constitutional right granted in several Latin America' countries, it does not exist as such in Canada's legal system. However, all Canadian provincial, territorial and federal

[45] Alberta: Freedom of Information and Protection of Privacy Act: http://www.qp.alberta.ca/574.cfm?page=F25.cfm&leg_type=Acts&isbncln=9780779743568; Health Information Act: http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest/rsa-2000-c-h-5.html; Personal Information Protection Act: http://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html. British Columbia: Freedom of Information and Protection of Privacy Act: http://www.oipc.bc.ca/legislation/FIPPA/Freedom_of_Information_and_Protection_of_Privacy_Act(April%202010).htm; Personal Information Protection Act: http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm; E-Health (Personal Health Information Access and Protection of Privacy) Act: http://www.oipc.bc.ca/legislation/E-HealthLegislation/E-Health%28PersonalHealthInformationAccessandProtectionofPrivacy%29Act.mht. Manitoba: Freedom of Information and Protection of Privacy Act: http://www.gov.mb.ca/chc/fippa/act_regulation.html; Personal Health Information Act: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php. New Brunswick: Right to Information and Protection of Privacy Act: http://www.canlii.org/en/nb/laws/stat/snb-2009-c-r-10.6/latest/snb-2009-c-r-10.6.html; Personal Health Information Privacy and Access Act: http://www.canlii.org/en/nb/laws/stat/snb-2009-c-p-7.05/latest/snb-2009-c-p-7.05.html; Newfoundland and Labrador: Access to Information and Protection of Privacy Act: http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm; Personal Health Information Act: http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm. Northwest Territories: Access to Information and Protection of Privacy Act. Nova Scotia: Freedom of Information and Protection of Privacy Act: http://nslegislature.ca/legc/statutes/freedom.htm; Part XX of the Municipal Government Act: http://www.gov.ns.ca/snsmr/muns/manuals/pdf/mga/mga20.pdf; Personal Information International Disclosure Protection Act: http://www.canlii.org/en/ns/laws/stat/sns-2006-c-3/latest/sns-2006-c-3.html. Nunavut: Access to Information and Protection of Privacy Act; Ontario: Freedom of Information and Protection of Privacy Act: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm; Municipal Freedom of Information and Protection of Privacy Act: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm; Personal Health Information Protection Act, 2004; http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm. Prince Edward Island: Freedom of Information and Protection of Privacy Act: http://www.gov.pe.ca/law/statutes/pdf/f-15_01.pdf. Québec: Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1_A.html; Act Respecting the Protection of Personal Information in the Private Sector: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html; An Act to amend the Act respecting health services and social services, the Health Insurance Act and the Act respecting the Régie de l'assurance maladie du Québec: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2008C8A.PDF; Saskatchewan: Freedom of Information and Protection of Privacy Act: http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf; Local Freedom of Information and Protection of Privacy Act: http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/L27-1.pdf; Health Information Protection Act: http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf; Yukon: Access to Information and Protection of Privacy Act: http://www.gov.yk.ca/legislation/acts/atipp.pdf.

laws applicable to the private or the public sector provide individuals with a right of access to their personal information, subject only to specific exceptions.

The *Privacy Act* and its regulation do include provisions for the access to and correction of personal information under the control of a government institution. Individuals are required to present a formal written request to the appropriate officer of the government institution which has control of their personal information. Informal requests can also be accepted however, individuals may not submit a complaint to the Privacy Commissioner for such requests since they are not done under the *Privacy Act.*

iv. Self Regulation:

The Canadian Standard Association's Model Code for the Protection of Personal Information (Q830) was developed in 1996 and has been approved as a National Standard of Canada by the Standards Council of Canada. It sets out ten principles that balance the privacy rights of individuals and the information requirements of private organizations and has been incorporated into the Personal Information Protection and Electronic Documents Act (PIPEDA). It continues to exist as self-regulatory tool independent of the PIPEDA and can be used as such by private sector organizations that are not subject to PIPEDA or to provincial legislation applicable to the private sector.[46]

B. Enforcement

i. Enforcement Mechanisms:

Enforcement mechanisms, regulations and procedures vary between Canadian provinces. Usually, an individual can complain to a provincial privacy commissioner and has a right to apply to the court. Nevertheless, the powers of the provincial privacy commissioners varies in each jurisdiction as does the right to go to court for review.

At the federal level, the Privacy Commissioner of Canada has the mandate of overseeing compliance with both the *Privacy Act* and the *Personal Information Protection and Electronic documents Act* (PIPEDA). She receives and investigates complaints regarding the application of these Acts. She may also initiate a complaint where there are reasonable grounds to investigate a matter under these Acts as well as conduct audits of the fair information practices of government institutions and of the personal information management practices of an organization. In order to do so, she might use her power to summon witnesses, administer oaths and compel the production of evidence. After, she must issue a report with recommendations to federal government institutions or private sector organizations to remedy situations, as appropriate. Her recommendations are not binding.

The *Privacy Act* provides a person who has been refused access to her/his personal information with a right to apply to the Court for review after the Privacy Commissioner has reported on her investigation. The Commissioner is allowed to apply and appear on behalf of such an individual, with his or her consent. With respect to the collection, use, disclosure, retention and disposal of personal information, the Privacy Commissioner can report her findings and recommendations

[46] http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code.

directly to a complainant and to Parliament when she believes that the Act has not been applied correctly by a government institution, but neither she nor the complainant is given the right, under the Act, to apply to Court to enforce her recommendations in this regard.

Under the PIPEDA, a complainant may, after receiving the Commissioner's report, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made. The Commissioner may also apply to the Court for a hearing. The Court is provided with the power to award damages and order an organization to change its practices as well as to report publicly on actions taken or proposed to be taken to correct its practices.

It should be noted that the implementation of the *Privacy Act* is also the responsibility of the President of Treasury Board, who is the designated Minister for the Act. As such, he is responsible for the preparation and distribution of directives and guidelines on the operation of the Act and the *Privacy Regulations*. The directives and guidelines are presently issued as mandatory Treasury Board Secretariat policy instruments in the form of a policy (*Policy on Privacy Protection*) and four directives (*Directive on Social Insurance Number, Directive on Privacy Practices, Directive on Privacy Impact Assessment, Directive on Privacy Requests and Correction of Personal Information*). The policy instruments include monitoring and reporting requirements in regards to the administration of the Act and Regulations. Compliance is monitored through public reporting documents, Treasury Board submissions, Departmental Performance Reports, results of audits, evaluations, studies and the Management Accountability Framework (MAF) for those institutions subject to this framework. They also include consequences that may be imposed should evidence of compliance issues be brought to the attention of the Treasury Board Secretariat and the President of the Treasury Board. The applicable consequences range from additional reporting requirements and recommendations to removal of delegated authority granted to heads of government institutions by the designated minister under the *Privacy Act*. Aside from the role of the President of the Treasury Board, as designated minister for the administration of the *Privacy Act* and *Privacy Regulations*, the responsibility to monitor compliance in individual government institutions rests first and foremost with the designated heads of the government institutions.

An unjustified breach of sections 8, 7 or 2(b) of the *Canadian Charter of Rights and Freedoms* can lead to remedial action under section 24 of the *Charter*. Subs. 24(1) invests a "court of competent jurisdiction" (judicially defined by a set of criteria) with the power to grant any remedy considered appropriate and just in the circumstances. Subs. 24(2) allows a court that concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by the *Charter* to exclude this evidence if it is established, having regard to all the circumstances, that its admission in the proceedings would bring the administration of justice into disrepute. In addition, pursuant to subs. 52(1) of the *Constitution Act, 1982*, any legislation or subordinate instrument that is judicially found to infringe s. 8, s. 7 or s. 2(b) of the *Charter* will be declared of no force or effect unless the state satisfies its burden to justify the restriction as a reasonable limit in a free and democratic society.

ii. Data Protection/Enforcement Authorities:

At the federal level, the main authority responsible for enforcing data protection laws is the Privacy Commissioner of Canada. The Commissioner is an agent of Parliament independent from the executive and the government institutions that are the subject of her investigations and audits. The Privacy Commissioner is appointed for a seven-year term by the governor in council after

approval by resolution of both Senate and House of Commons. The Commissioner holds office during good behavior and may only be removed on address of the Senate and House of Commons. The Commissioner is to "engage exclusively in the duties of the office of Privacy Commissioner" and reports annually on the activities of the office to Parliament but may also report more frequently in urgent situations. Her appointment may be renewed at the end of the seven year period. The Office of the Privacy Commissioner has a staff of approximately 176 employees and an annual budget of approximately $24 million (CAN).[47]

The Privacy Commissioner of Canada received an average of 750 complaints per year over the last 5 years related to the Privacy Act and about 330 per year over the last 5 years related to the Personal Information Protection and Electronic Documents Act (PIPEDA).[48]

Under the Privacy Act, the Privacy Commissioner shall receive and investigate each complaint. Under the PIPEDA, she is authorized to deal in a more summary fashion with some complaints. Indeed, she is permitted to refuse to investigate a complaint if, for example, the complaint ought first to be addressed under other grievance or review procedures reasonably available, or if it would be more appropriately handled through procedures established under another law. As well, the Privacy Commissioner may discontinue investigations in certain limited circumstances, including when she is of the opinion that there is insufficient evidence to proceed, the complaint is trivial, frivolous, vexatious, or made in bad faith, and that the matter is already the subject of an ongoing investigation, etc.

At the provincial level, each province and territory, an independent privacy commissioner is primarily responsible for enforcing data protection laws but its size in terms of staff and budget vary broadly.[49]

Under the *Privacy Act*, the Privacy Commissioner and every person acting on behalf or under her direction shall keep confidential information that comes to their knowledge in the performance of their duties and functions. The Commissioner is nevertheless authorized to disclose that information if this is, in her opinion, necessary to carry out an investigation following the Act.

---

[47] Privacy Commissioner of Canada: http://www.priv.gc.ca/

[48] Annual Report on the Personal Information and Electronic Documents Act (2010): http://www.priv.gc.ca/information/ar/201011/2010_pipeda_e.pdf; Annual Report on the *Privacy Act* (2010-2011): http://www.priv.gc.ca/information/ar/201011/201011_pa_e.pdf.

[49] Office of the Information and Privacy Commissioner of Alberta: http://www.oipc.ab.ca/pages/home/default.aspx; Office of the Information and Privacy Commissioner for British Columbia: http://www.oipc.bc.ca; Ombudsman of Manitoba : http://www.ombudsman.mb.ca; Access to Information and Privacy Commissioner of New Brunswick: http://www2.gnb.ca/content/gnb/en/contacts/dept_renderer.201145.html; Information and Privacy Commissioner of Newfoundland and Labrador: http://www.oipc.nl.ca; Information and Privacy Commissioner of the Northwest Territories: http://www.commissioner.gov.nt.ca/privacy; Nova Scotia Freedom of Information and Protection of Privacy Review Office: http://www.foipop.ns.ca; Information and Privacy Commissioner of Nunavut: http://www.info-privacy.nu.ca; Office of the Information and Privacy Commissioner of Ontario: http://www.ipc.on.ca/english/Home-Page; Information and Privacy Commissioner of Prince-Edward Island: http://www.assembly.pe.ca/index.php3?number=1013943; Commission d'accès à l'information du Québec: http://www.cai.gouv.qc.ca/index-en.html; Information and Privacy Commissioner of Saskatchewan: http://www.oipc.sk.ca; Information and Privacy Commissioner of Yukon: http://www.ombudsman.yk.ca/privacy/ipchome.html.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) prohibits the Privacy Commissioner of Canada or any person acting on her behalf from disclosing any information that comes to their knowledge as a result of the performance of her duties or powers under the Act. The Privacy Commissioner may however make public information about the management practices of an organization if the Commissioner believes that it is in the public interest to do so.

The Privacy Commissioner is permitted to disclose certain information to her foreign counterparts provided that these counterparts have, under the laws of a foreign state, 1) functions and duties similar to those of the Privacy Commissioner in respect of the protection of personal information and 2) responsibilities with respect to addressing conduct that would be considered to contravene PIPEDA.

This information must be 1) relevant to an ongoing or potential investigation of a contravention of the foreign law, provided that the conduct being investigated is substantially similar to that which would be in contravention of PIPEDA or; 2) necessary to disclose in order for the Privacy Commissioner to obtain from her foreign counterpart information that would be useful to an investigation or audit under PIPEDA.

The Privacy Commissioner can only disclose information to her foreign counterparts if she has entered into a written arrangement.

iii. Remedies/Recourse:

Recourse: In several Canadian provinces, the tort of invasion of privacy has been created by legislation. The right to privacy also exists in the Civil Law of Quebec. In these provinces, individuals are then provided with recourse for harm caused by privacy violations. In the other common law provinces, the recourse depends on the potential recognition of a privacy tort by the courts. Recently, the Ontario Court of Appeal has opened the door to such a recourse by recognizing a privacy tort of "intrusion upon seclusion" (see Jones v. Tsige, (2012) ONCA 32.)
At the federal level, the Personal Information Protection and Electronic Documents Act expressly permits the Court to order damages to the complainant, including damages for any humiliation that the complainant has suffered.[50]

Recourse for harm caused by privacy violation by a federal institution is not expressly established by the Privacy Act. Consequently, such recourse depends on the potential recognition of a privacy tort by the courts.

As set out in the previous sub-question, the Charter contains internal remedial provisions. An individual could have recourse under section 24 of the Charter in cases where the right guaranteed by sections 8, 7 or 2(b) has been infringed. Among the possible remedies ordered are damages and the exclusion of evidence obtained in violation of constitutional rights. Similarly, when legislation is inconsistent with the Charter, it can be declared of no force or effect pursuant to subs. 52(1) of the Constitution Act, 1982.

[50] Nammo v. TransUnion of Canada Inc., (2010) FC 1284; Girao v. Zarek Taylor Grossman Hanrahan LLP, (2011) FC 1070 and Landry v. Royal Bank of Canada, (2011) FC 687)

Authority to enforce data protection: As mentioned before, the provincial and federal legislations are enforced through Parliaments, privacy commissioners and the courts. See our answer at question IIA for the description of the enforcement models at the federal level.

iv. Investigatory Capabilities/Criminal Prosecution:

Under the Privacy Act, the Privacy Commissioner of Canada is empowered to receive complaint from an applicant on issues ranging from the use and disclosure of personal information to the right of access to personal information by individuals to whom it pertains. If the Privacy Commissioner is satisfied that there are reasonable grounds to investigate one of these issues, she may initiate a complaint. She may also, from time to time at her discretion, carry out investigation in respect of personal information under the control of government institutions to ensure compliance with provisions related to the collection, use and disclosure of personal information. Following her investigation, she will issue a report containing her findings and any recommendation that she considers appropriate.

Under the Personal Information Protection and Electronic Documents Act (PIPEDA), the Privacy Commissioner of Canada may, in addition to her power to investigate complaints as described under D above, initiate a complaint if she is satisfied that there are reasonable grounds to investigate a matter under the Act. The Privacy Commissioner has one year to file a report of a complaint that she has initiated. The report must to contain the Privacy Commissioner's findings and recommendations, a notice of settlement reached by parties and, if appropriate, a notice of any action taken or proposed to be taken to implement the Privacy Commissioner's recommendations. The Privacy Commissioner may also audit the personal information management practices of an organization if the she has reasonable grounds to believe that the organization is contravening the Act. After an audit, the Privacy Commissioner is required to provide the organization with a copy of the audit report containing the findings of the audit and any recommendations she considers appropriate. The audit report may also be included in the Privacy Commissioner's annual report to Parliament.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not include criminal sanctions. However, under the Act, the Privacy Commissioner may disclose information in the course of a prosecution for an offence of perjury under the *Criminal Code of Canada* in respect of a statement made under PIPEDA. The Privacy Commissioner may also disclose to the Attorney General of Canada or to the provincial Attorney Generals information relating to the commission of an offence against any law of Canada or a province, if it is the Commissioner's opinion that there is sufficient evidence to do so[51].

C. Cross-Border Cooperation

i. Data Transfer:

At the federal level, the rules are different depending on whether the Privacy Act or the Personal Information Protection and Electronic documents Act (PIPEDA) is applicable. The Privacy Act

[51] Criminal Code sections 56.1, 368(1) and 402.2 regarding identity theft and related misconduct: http://laws-lois.justice.gc.ca/eng/acts/C-46.

does not establish special rules or conditions for the disclosure of personal information to other countries. The same specific and limited rules governing the disclosure of personal information to third parties applicable in the domestic context are also applicable to disclosures made to other countries. The Federal Government, however, has issued a guidance document to institutions subject to the Privacy Act which includes a privacy checklist and advice on considering privacy prior to initiating contracts, in particular, those that involve transborder data flows.[52]

The PIPEDA contains an accountability principle that makes an organization accountable for the personal information in their control or custody, including personal information that they have transferred to a third party for processing. Organization subject to PIPEDA are required to use contractual or other means to ensure that the information that they have transferred to a third party for processing will receive, from the third party processor, a level of protection comparable to that established under PIPEDA. This requirement applies whether the processor is in Canada or abroad.

At the provincial level the disclosure of personal information held by provincial or territorial government institutions to other countries is regulated by provincial or territorial statutes. The limits or conditions on such transfers vary from province or territory to another.

ii. International Instruments/Arrangements:

Canada signed OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1984. Both statutes regulating protection of personal information at the federal level, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA), were adopted to follow the OECD guidelines.

Canada is an APEC member since 1989. It endorsed the APEC Privacy Guidelines in 2004 and the APEC Cross Border Privacy Rules System in 2011. The Office of the Privacy Commissioner of Canada joined with privacy enforcement agencies around the world in September 2010 to establish the Global Privacy Enforcement Network (GPEN). The Office of the Privacy Commissioner of Canada is also a participant in the APEC CPEA

In December 2001, the European Commission ruled that Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) received an "Adequacy Finding", meaning that it meets the standards for the protection of personal data as outlined in the European Union's Data Protection Directive. This decision was confirmed in 2006 following the assessment of the Canadian compliance with the 2001 adequacy decision.[53] In 2005, the protection of personal data

---

[52] Guidance Document: Taking Privacy into Account Before Making Contracting Decisions: http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcptb-eng.asp

[53] Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act" http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0002:en:NOT;
The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-5.

contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency was also considered adequate.[54]

ii. Cross-Border investigatory and enforcement cooperation:

Cross-border collaboration exists between specific Canadian federal institutions and counterparts in foreign countries.

The Privacy Commissioner of Canada collaborates with counterpart authorities in certain investigations the transfer of personal information across international borders. The Privacy Commissioner is a founding member of Global Privacy Enforcement Network (GPEN), a network designed to facilitate the sharing of information about issues related to enforcement and collaborative outreach activities. The Privacy Commissioner is also a participant in the APEC Cross Border Privacy Enforcement Arrangement (the APEC CPEA), which provides mechanisms to facilitate cross-border cooperation in the enforcement of privacy laws, including facilitating the contact between CPEA participants for the purpose of seeking assistance or making referrals regarding privacy investigations and enforcement matters.

In addition, police authorities cooperate with other governments as needed in matters respecting the enforcement of *Criminal Code* provisions regarding the theft of identity and other specific infractions relating to data protection issues.

D. Case Law and Special Challenges

At the provincial and federal levels, the protection of personal information is largely regulated by statutes. Consequently, the law regulating individual privacy protection is highly influenced by judges either in the context of judicial review applications challenging government decisions, or in the context of the interpretation of the statutes creating the privacy protection regimes.[55]

Judicial rulings regarding the scope and the application of the section 8 of the Charter play certainly a capital role in the protection of individual's privacy in Canada.[56]

---

[54] Commission decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-5.

[55] Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R. 403; H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General), [2006] 1 S.C.R. 441; Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police), [2003] 1 S.C.R. 66: http://csc.lexum.org/en/2003/2003scc8/2003scc8.html.

[56] Hunter v. Southam Inc., [1984] 2 S.C.R. 145: http://csc.lexum.org/en/1984/1984scr2-145/1984scr2-145.html; R. v. Dyment, [1988] 2 S.C.R. 417: http://scc.lexum.org/en/1988/1988scr2-417/1988scr2-417.html; R. v. Plant,[1993] 3. S.C.R. 281: http://scc.lexum.org/en/1993/1993scr3-281/1993scr3-281.html; R. v. Colarusso, [1994] 1 S.C.R. 20: http://scc.lexum.org/en/1994/1994scr1-20/1994scr1-20.html; Smith v. Canada (Attorney General), [2001] 3 S.C.R. 902: http://scc.lexum.org/en/2001/2001scc88/2001scc88.html; R. v. Law, [2002] 1 S.C.R. 227: http://scc.lexum.org/en/2002/2002scc10/2002scc10.html; R. v. Tessling, [2004] 3 S.C.R. 432: http://scc.lexum.org/en/2004/2004scc67/2004scc67.html; R. v. Rodgers, [2006] 1 S.C.R. 554: http://scc.lexum.org/en/2006/2006scc15/2006scc15.html; R. v. Kang-Brown, [2008] 1 S.C.R. 456: http://scc.lexum.org/en/2008/2008scc18/2008scc18.html; R. v. A.M., [2008] 1 S.C.R. 569: http://scc.lexum.org/en/2008/2008scc19/2008scc19.html; R. v. Patrick, [2009] 1 S.C.R. 579:

The development of new technologies, in particular the computer with its virtually limitless power to collect, use, disseminate and retain data, was the key policy driver in the adoption of both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Both Acts were drafted in a technology-neutral fashion and, as such, it has been possible to find ways of applying the privacy protection principles to new technologies and services that have developed since the laws were adopted.

3. Colombia:

Colombia provided a response to the CJPA's Questionnaire on Privacy and Data Protection Legislation and Practices. This response is contained in document CP/CAJP-3026/11 add. 10 and provides the foundation for the information summarized in the present section.[57]

A. Legal Context

i. Constitutional Framework:

The Colombian constitution of 1991 establishes that: all people are entitled to their personal and family privacy and good name, and that the State must respect that right and ensure respect thereto. Similarly, all people are entitled to access, update, and rectify information gathered about them in public and private files and databases.[58] It also guarantees everyone's right to freedom to expression and to disseminate his/her thoughts and opinions, to transmit and receive truthful and impartial information, to establish mass media, and ensure that there will be no censorship. The constitution also establishes that these are free and have a social responsibility and provides for the right to rectification under equitable conditions.[59] Moreover, since both of the right to privacy and the right to freedom of expression are enshrined in Chapter I of the Constitution on fundamental rights, they are immediately applicable.[60]

ii. Legislative Framework:

The Colombian Legislature passed the Statutory Law containing "general provisions for the protection of personal data," on December 16, 2010 (the "new law"). Enactment requires review by the Constitutional Court, which occurred on October 6, 2011,[61] as well as the written resolution of the court and sanctioning by the President. These final two steps, although expected, have not been completed as of the date of this report.

---

http://scc.lexum.org/en/2009/2009scc17/2009scc17.html; R. v. Gomboc, [2010] 3 S.C.R. 211: http://csc.lexum.org/en/2010/2010scc55/2010scc55.html.

[57] The Colombian Congress passed the law on the protection of data in December 2010, the implementation of which requires review by the Constitutional Court to become operational. Said Court ruled on its constitutionality on October 6, 2011, but as of the date of this report had not delivered its final resolution, which is in turn is necessary before the law can be sanctioned by the President. The answers to the questionnaire and content of the present section are therefore limited exclusively to the text of the law. Case law and practical/regulatory features regarding the operation of the law do not exist as of the date of the present report .

[58] Constitution Article 15.

[59] Article 20

[60] Article 85 Constitution

[61] Constitutional review in Case C-748-2011.

The legislature also amended the Criminal Code to create a new legally protected matter "protection of information and of data." This law establishes new criminal offenses related to computer crime, the protection of information and the protection of personal data protection, with imprisonment of up to 120 months and fines of up to 1500 monthly legal minimum wage.[62]

The law specifically sanctions the violation of personal data when a person/entity, without being authorized to do so, and with advantages for oneself or to a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or uses personal codes, personal data contained in files, registries, databases or similar media, punishable with imprisonment of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 monthly legal minimum wage.

Colombia also enacted Law 1266 (2008), which dictates the general provisions of habeas data and regulates the handling of the information contained in databases of personal data, especially financial, credit, trade, and services information, as well as information from third countries.[63] Finally, Law 79 (1993) regulates the Census process on a national basis and establishes procedures for processing of personal data in that context.

Law 1266, 1273 and the recently approved law on data protection apply to both public and private sectors. Law 79 applies exclusively to the public sector census agency.

[62] Law 1429 of 2010.
[63] In its review, the Constitutional Court determined law 1266 was sectoral in nature and confined it exclusively to the processing of data related to credit risk analysis (Case C-1011).

iii. Habeas Data:

At the constitutional level, as mentioned in subsection (i) above, the right commonly known as "habeas data," establishes that individuals are entitled to their personal and family privacy and good name. The State must respect that right and ensure that it is respect by others. The individual is also entitled to access, update, and rectify information gathered about him/her in public and private databases and files.[64]

At the statutory level, the new data protection law makes operational the constitutional right of all individuals to access, update and correct personal information in databases or files, be they public or private.[65] Moreover, the Constitutional Court in its review of the law held that the constitutionality of the new data protection law establishes that individuals have the right to delete such information, creating a resemblance to ARCO rights: rights to access, rectification, cancelation and opposition to the processing of personal data.[66]

iv. Self Regulation:

The new data protection law permits the development of self-regulatory or self-control schemes or systems, such as binding corporate rules. Such system would be subject to regulations issued by the Government at a future date in order to certify good practice in data protection and transfer of information to third countries.[67]

B. Enforcement

i. Enforcement Mechanisms:

The main mechanism for enforcement is contained in Decree 2591 of 1991 and the previously mentioned data protection provisions. Law 1266 (2008) and the new law on data protection, also establish an administrative procedure to access (or consult) the personal data processed by the controller or processor, as well as an administrative appeals procedure which proceeds directly to the supervisory authority. To exercise the latter, it is necessary to have first undertaken the procedure to access/consult the personal data, in order that the individual consider whether a possible violation has occurred in the processing of his/her information.

In part, the new data protection law provides that individuals may consult and have access to his/her personal information in any public or private sector database. The consultation shall be made via the procedure provided for by the data processor, which will have a maximum of ten (10) working days from the date of receipt thereof. When it is not possible to satisfy the consultation request within that term, the processor shall inform the individual of the reasons for the delay and indicate the date on which the request will be complied with. In any case, this latter term cannot exceed five (5) working days following expiration of the first term.[68]

---

[64] Constitution Article 15,
[65] New law, Article 1.
[66] Constitutional Court judgment C-748 of 2011.
[67] New Law, Article 28.
[68] "Article 14.

ii. Data Protection/Enforcement Authorities:

In Colombia there are currently two administrative authorities responsible for the enforcement of laws and regulations on privacy/data protection: (i) the Superintendency of Industry and Commerce; and (ii) the Financial Superintency of Colombia.

The Superintendency of Industry and Trade is a technical body, attached to the Executive Branch of the Public Ministry of Trade, Industry and Tourism, whose functions include compliance with consumer protection rules, protection of personal data, compliance with antitrust/competition rules, management of the national industrial property system, as well as jurisdictional issues concerning consumer protection and unfair competition.[69] Within this Superintendency, the Section for the Protection of Personal Data shall carry out the enforcement in the processing of personal data.[70] The Superintendency of Industry and Trade counts with 599 officials and its budget for 2012 was $56.396.350.000 (Colombian pesos) for its operations and $13.242.180.000 (Colombian pesos) for investment.

The Financial Superintencency of Colombia is a technical body, attached to the Executive Branch of the Public Ministry of Finance, responsible for overseeing the operation of financial markets and Colombian stock exchange, to preserve its stability, security and trust, and to promote, organize and develop the securities market and protect investors, depositors and policyholders.[71]

In general terms, the Superintendency of Industry and Trade individually addresses complaints presented to it by individuals and determine, based on the same, if the case merits opening an administrative investigation. However, it should be noted that the Superintendency also with broad powers to issue instructions, conduct external audit inspections or undertake an official investigation at its own initiative.

The volume of complaints addressed by the Superintendency of Industry and Commerce regarding the violation of data protection rules and in particular with the provisions of Act 1266 of 2008 is as follows: 654 in 2009; 1058 in 2010; 1725 in 2011; 228 (January to March) 2012. The total as of the date of this report was 3665.

iii. Remedies/Recourse:

The individual, who considers that personal data contained in a private or public database should be corrected, updated or deleted, may file a complaint with data processor. Said claim shall be in writing, identify the individual title-holder of the information, and describe the facts that give rise to the claim. After receiving the completed claim, the date processor must make a notation of "pending claim" in the database and must address the claim within fifteen (15) working days from receipt.[72] If after this process is completed, the individual considers that the claim has not been addressed properly, he/she may submit the complaint to the Superintendent of Industry and Trade.[73]

---

[69] Decree 4886 of 2011

[70] The Section for Personal Data Protection was incorporated into the structure of the Superintendency of Industry and Trade by Decree 4886 of 2011.

[71] Staff and Budgetary figures for the Financial Superintendency were not provided.

[72] Article 15.

[73] Article 16

Law 1266 also establishes several obligations to the Superintendency of Industry and Commerce related to privacy/data protection, including requirements: to issue instructions and orders on how data processors should comply with the privacy/data protection law, rules and regulations; to oversee and ensure compliance with data protection laws, rules and regulations, as well as orders issued by the respective Superintendency; to ensure that data processors count with sufficient security and technical capabilities to ensure personal data is not altered, lost, accessed in unauthorized manner, or used in violation to the law; to arrange external audits to monitor compliance with the provisions of the law by data processors; to require, on its own motion or upon request of an individual, the modification or removal of personal data when appropriate, in accordance with the provisions of the law; to commence, on its own motion or upon request of an individual, an administrative investigation against processors, sources and users of financial, credit and trade information, as well as services from third countries; to establish whether a processor has incurred in administrative liability arising from breach of the provisions of the law or non compliance with orders or instructions issued by the relevant supervisory body; and, if appropriate, to impose sanctions or order the measures relevant to the enforcement of privacy/data protection rights.[74]

iv. Investigatory Capabilities/Criminal Prosecution:

As discussed above, Law 1266 Act allows enforcement authorities to initiate ex-officio and ex-parte investigations. Criminal proceedings are a matter for the Attorney General's Office. On the topic, Law 1273, amending the criminal code creates a new legally protected tutelage, titled "protection of information and data." This requirement is contained into two chapters of the criminal code: one chapter against attacks to the confidentiality, integrity and availability of data and computer systems and from the computer attacks and other breaches; and a second chapter that establishes the relevant criminal offenses relating to the protection of personal data.[75]

With regard to the violation of personal data, the code provides that a person/entity not authorized to do so, advantages oneself or a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies, or uses personal codes, or personal data contained in files, registries, databases or similar media, may be punished with imprisonment of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 monthly legal minimum wage.

In this regard it is important to note that Act 1266 defined the term personal data as "any piece of information linked to a person or persons identified or identifiable or that may be associated with a natural or legal person." This article requires special care by data processors in the handling of personal data of their employees, since the law requires anyone who "breached" or "intercepts" the data to seek authorization from the title-holder of the data.[76]

C. Cross-Border Cooperation

i. Data Transfer:

The new data protection law prohibits transfer of personal data to countries that do not provide adequate levels of data protection as determined by the Superintendency of Industry and

[74] Law 1266 of 2008, artcile 17.
[75] Colombian Criminal Code Title VII BIS
[76] Section 269F: violation of personal data

Commerce. In no case can the standard of the recipient be lower than the standard required by the Colombian law.[77]

ii. International Instruments/Arrangements:

Participation in international instruments and arrangements, although possible under the new law, has not occurred formally at this time. However, Colombia is part of the Ibero-American Network Data Protection and through this forum has participated in the exchange of information, concerns, and suggestions regarding the latest issues concerning data protection at both global and Latin American level.

Colombia has not received certification by the European Union. Colombia requested the European Commission to begin the process of adaptation in 2009, but it was suspended pending the drafting and adoption of the new law on data protection. It is estimated that Colombia will again request initiation of the process in April 2012.

ii. Cross-Border investigatory and enforcement cooperation:

The new data protection establishes that the data protection authority shall request the collaboration from international or foreign entities when they affect the rights of Colombian individuals.[78] And although the new law establishes cross-border collaboration, the Law has not yet been enacted and, thus, this power has been exercised by the authority in practice.

D. Case Law and Special Challenges

Since 1992, the Constitutional Court of Colombia has issued approximately 70 thematic statements regarding the protection of personal data.[79] Some of the major issues considered by the Court include: human dignity and privacy under the Constitution of 1991; the legal effect of new technology on personal freedom; privacy and habeas data and the application of Article 15 of the Constitution; the correlation between privacy and right of access to information; data as "property;" databases and constitutional law; the expiration of personal data; the increasing computerization and inadequate legal and social protections; the responsible use of information, etc. Of the most significant challenges mentioned as Colombia moves toward the implementation of it new law on data protection include cloud computing and cross-border flows of information.

4. Costa Rica:

Costa Rica provided a response to the CJPA's Questionnaire on Privacy and Data Protection Legislation and Practices. This response is contained in document CP/CAJP-3026/11 add. 6 and provides the foundation for the information summarized in the present section

[77] Article 26. The law establishes exceptions for cases in which the individual consented to the transfer; for the exchange of medical data required for treatment or public health; for stock exchange or banking transfers; as agreed in international treaty; to safeguard the public interest or for the establishment, exercise or defense of a right in a judicial proceeding.

[78] Article 21

[79] This extensive case law is summarized in the table contained in Section III of Colombia's response to the Questionnaire on Privacy/Data Protection, Document CP/CAJP-3026/11 add. 10, available at: http://www.oas.org/dil/esp/proteccion_de_datos_cuestionario_Colombia.pdf.

A. Legal Context

i. Constitutional Framework:

The Constitution of Costa Rica of 1949 establishes the right to privacy, to freedom and to secrecy of communications. According to article 24, the private documents and written communications (oral or otherwise) of the inhabitants of the Republic are considered inviolable. The scope of this provision covers various forms of private life (economic, commercial, financial, and professional) and may be disclosed to third parties only if there is a clear public interest in that information. The existence of this public interest is the element that distinguishes between public information, which is generally accessible and, private information, which must be declared confidential.[80]

The right to freedom of expression is included in article 28 of the Constitution and guarantees that no person may be disturbed or persecuted for the expression of his/her opinions or for any act that does not violate the law. Similarly, article 29 provides that all citizens can communicate their thoughts orally or in writing, and publish without prior censorship, but making them responsible for abuses committed in the exercise of this right.

Informational self-determination is a right that has been born with the advent of information technology and communications. As a result, unlike other countries, the Costa Rican Constitution of 1949 does not include provisions dealing specifically with privacy/data protection or habeas data. It is important to note, however, that academics, judges and legal practitioners attempt to interpret the constitutional articles mentioned above for the protection of privacy and intimacy, in order to support for the right to informational self-determination (data protection and habeas data), the scope of the former rights is more extensive and important than of the latter.

[80] Article 24

ii. Legislative Framework:

Comprehensive Legislation: Costa Rica adopted Law No. 8968 on July 7, 2011 on the "Protection of the individual against the Processing of Personal Data," which applies at the national level (including national, county and municipal level), to both public and private sectors. The law seeks to gather internationally recognized principles on informational self-determination, establish a broad scope of application, and provide definitions of the different protected elements. It also includes basic principles and rights concerning protection of personal data, such as explaining the content of informational self-determination, the principles of informed consent, the obligation to inform the citizen, the need for consent, some exceptions to informational self-determination, develops the principle of quality of information, which includes the topicality, correctness, accuracy, and proportionality for collection purposes.

The law also covers other rights granted to citizens, such as access to information (which includes the regular varieties of knowledge about the existence of personal data in public or private databases) and the right of correction/rectification. It also defines the different categories of data, such as what is defined as sensitive data, personal data subject to restricted access, personal data subject to unrestricted access and data on credit reporting.

The law also regulates the security and confidentiality in the treatment of data and protocols for the procedures to be followed in the collection, storage and handling of personal data, as well as the necessary safeguards to protect against acts that violate the fundamental rights of citizens. It also make reference to the transfer of personal data, as general rule permitting its transfer only when the right holder has expressly and validly authorized such action and this is done without violating the principles and rights under this law.

Sectoral Legislation: There are also sectoral rules related to privacy/data protection, including: the General Telecommunications Law No.8642 that addresses the privacy of communications and protection of personal data that may be in the hands of companies which provide telecommunications services and which requires such companies have the technical features necessary to ensure the security of networks and services, the right to privacy and protection of personal data of subscribers;[81] the Regulation to the General Telecommunications Law, which governs all operators or telecommunications service providers to ensure the secrecy of communications, the right to privacy and protection of the personal data of users;[82] the Law Regulating Insurance Contracts No.8956, which provides protection to the data collected, and establishes the requirement that insurance companies, subsidiaries, ancillary service providers, subcontractors and their personnel, uphold a duty to protect confidentiality of the personal data that is collected during the course of their operations;[83] the Costa Rican Refugee Regulations, which establish the principle of confidentiality regarding the recording and processing of information on refugees;[84] the Regulation for Universal Access, extends the protection recognized in the General Law of Telecommunications to beneficiaries of the National Telecommunications Fund;[85] the Judicial Policy for Improving Access to Justice for Women, Children, and Adolescents in Costa Rica, which includes provisions to safeguard the right of these individuals to dignity and privacy/data protection;[86] and the Guidelines to reduce victimization of Children and Adolescents in Disability status judicial, which requires that judicial authorities protect the privacy of vulnerable persons in judicial proceedings.[87]

In addition, Costa Rica has also signed international treaties on various subjects which required enacting sectoral-type legislation which contain rules on privacy/data protection. Examples include the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, which establishes the obligation of States to protect the privacy and identity of child victims at all stages of criminal proceedings;[88] Agreement with French Government for Readmission of Irregular Migrants, which requires that the personal data of the readmitted individual be treated and protected pursuant to the data protection in force in each State;[89] and the International Convention for the Protection of all Persons from Forced Disappearances, which states that a person under judicial custody is entitle to privacy/data protection when divulging such data may harm his/her privacy, among others.[90]

Costa Rica is also signatory to the Standard Minimum Rules for the Dissemination of Judicial Information, the so-called "Heredia Rules," a declaration approved at the Internet and Judicial System Seminar held in the city of Heredia (Costa Rica), 8 and 9 July 2003 with the participation

---

[81] Ley General de Telecomunicaciones No.8642 (4 de junio de 2008), *Articulo 42 y 43.*
[82] Reglamento sobre Medidas de Protección de la Privacidad en las Comunicaciones, decreto ejecutivo No.35205 de 16 de abril de 2009.
[83] la Ley Reguladora del Contrato de Seguros No.8956 del 17 de junio de 2011, Artículo 21.
[84] Decreto ejecutivo No.36831 de 28 de setiembre de 2011, en su artículo 8,
[85] Reglamento de Acceso Universal, Servicio Universal y Solidaridad de 6 de octubre de 2008, *Artículo 28*
[86] Norma del Poder Judicial, en la Circular No.63 de 31 de mayo de 2011.
[87] Circular 168 de 7 de diciembre de 2010
[88] Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía, aprobado mediante ley No.8172 de 7 de diciembre de 2001, Artículo 8.
[89] Ley No.7993 de 7 de marzo de 2000, Articulo 8.
[90] Ley No.9005 de 31 de octubre de 2011, artículo 20

of judiciary, civil society organizations and academics from Argentina, Brazil, Canada, Colombia, Costa Rica, Ecuador, El Salvador, Mexico, Dominican Republic and Uruguay, are a series of ten recommendations five statements, and definitions, to assist the judiciaries of signatory countries adopt dissemination practices and web-based application for the public to consult information concerning the docket and decisions of the courts. These rules promote the broader dissemination of information, but require it be fully consistent with the principles of informational self-determination and privacy/data protection.

Finally, it is also necessary to note that Costa Rican law provides a definition for what is meant by private documents. In this sense, Costa Rica adopted the Law on Registration, Seizure and Examination of Private Papers and Intervention of Communication, derived directly from Constitutional Article 24, which states that the following are considered private documents: written correspondence, fax, telex, data transmission or any other means, videos, cassettes, tapes, disks, diskettes, writings, books, memorials, records, plans, drawings, paintings, radiographs, photographs and any other form of recording information of private character, used with declarative or representative intent, to illustrate or prove something.[91]

iii. Habeas Data:

As described above, Costa Rican law provides a regulated procedure which corresponds to a process referred to as habeas data, so that citizens can access their personal data held in any database. The aforementioned law guarantees the rights granted to the individual who considers that their rights and privileges as to informational self-determination have been broken, so as to permit said individual to access, rectify and/or remove the information.[92]

iv. Self Regulation:

Codes of conduct (professional ethics) are relatively common in various professional associations and seek a type of self-regulation in matters within their competency. However, in terms of informational self-determination, there are no codes of conduct that directly affect privacy/data protection. Perhaps the only example where the private attempts guarantees privacy/data protection, although not expressly informational self-determination, is the Association of Journalists of Costa Rica, which issued a Code of Ethics for professionals that requires journalists behave in a respectful manner in obtaining information with respect to others' pain, privacy and intimacy,[93] and that requires journalist respect the right to privacy of the socially vulnerable persons and legal entities.[94]

For others, there is no code of similar nature which applies to privacy/data protection or which seeks to respect informational self-determination. However, the private sector must adjust its actions to comply with the positive legal norms mentioned above.

---

[91] Law on Registration, Seizure and Examination of Private Papers and Intervention of Communication No.7425, 09 August 1994.
[92] Law No. 8968 of July 7, 2011, Article 7
[93] Regulation No.158 of 16 August 2011, paragraph 24
[94] Article 38

B. Enforcement

i. Enforcement Mechanism:

The new law requires the establishment of an enforcement procedure and creation of the Data Protection Agency for Residents (Prodhab). The Prodhab, which is still in its strategic planning stages, will function on the principle of denunciation whereby any individual who considers his/her rights to privacy/data protection violated in any way, by public or private sector actors, may raise a claim before Prodhab.[95] Upon receipt of a complaint, the data processor, within three business days shall provide a sworn statement on the veracity of such charges and provide any evidence to support its position. In cases where said statement is not provided to the Prodhab within the three-day timeframe, the claims of the accusing party shall be considered accurate.[96]

At any time, Prodhab may order the data processor to provide any necessary information and may conduct on-site inspections directly. In addition, Prodhab may also order precautionary measures to ensure the effective outcome of the procedure and to safeguard the rights of the individual. Prodhab shall issue a final resolution within one month after the filing of the complaint. Resolutions of Prodhab are subject to appeal within the three days of final resolution, and must be resolved within eight days after presentation of said appeal.

For cases in which Prodhab determines that the personal data subject to the complaint false, incomplete, inaccurate, or that in accordance with the rules on protection of personal data was collected, stored or disseminated improperly, Prodhab shall order the immediate removal, correction, addition or amendment, or shall stop its transfer or dissemination. If the person obligated to comply with the resolution does not fully satisfy the order, it will be subject to the penalties provided in the data protectionand other laws.[97]

Prodhab may also initiate proceedings ex-officio or ex-parte to determine whether a database regulated by the data protection law is being used in accordance with its principles and issue binding resolution.[98] The resolution is subject to appeal within three days of its issuance.[99] Temporarily, while Prodhab is transitioning toward operation, the channel through which an individual may protect his/her privacy/data protection is by filing an amparo before the Constitutional Court, the body which has previously had jurisdictional authority to resolve issues concerning privacy/data protection.[100]

ii. Data Protection/Enforcement Authority:

Law No. 8968 requires the creation of the Agency for Data Protection of the Citizen ("Prodhab"), which will be a body under the Ministry of Justice and Peace, will enjoy a fully legal and instrumental decentralization in carrying out the duties assigned to it, and will manage its own

[95] Artcile 24
[96] Article 25
[97] Article 26 states that
[98] Database audits will be regulated pursuant to the General Law of Public Administration.
[99] Prior to the final standardization of procedures under the new data protection law, all matters not expressly provided by law shall be subject to the provisions of Book II of the General Law of Public Administration No. 6227 of May 2, 1978.
[100] Law on Data Protection Article 29 and Constitutional Jurisdiction Act No.7135, 11 October 1989

resources and budget. The Prodhab will have faculty to sign contracts and agreements required for the fulfillment of its duties and will have independent in its judgment.[101]

The allocation of human resources can yet be established, but shall comprise the technical and administrative personnel necessary for the proper performance of its duties. Staff will be appointed by competition, according to the Civil Service Charter or as provided in the regulations to the law, which has not yet been issued.[102]

Following adoption of the law, agreement No.212 of 22 November 2011 was reached, declaring that the creation of Prodhab is of public and national interest. The text of agreement states that a Commission shall be established in charge of the creation of Prodhab, to coordinate, plan and define all aspects necessary for the proper implementation of said Agency. The Commission shall consist of the General Counsel of the Ministry of Justice and Peace, Legal Director of the National Register, a representative of the Office of the Minister of Justice and Peace, a representative of the Office of Consumer Advocacy, a representative of the Ministry of Science and Technology, a representative of the Ministry of Foreign Trade, a representative of the Office of Public Ethics, as well as a representative of the Ombudsman of the Republic (as an observer). The Commission will be coordinated by the General Counsel of the Ministry of Justice and Peace.

Moreover, the Commission in charge of creating Prodhab is also responsible for drafting the Regulation to the new Law on Data Protection, which should be completed in a maximum of 6 months from the implementation date of Prodhab. It is also noted that agencies and institutions of public and private sector may contribute expertise in the creation of the Prodhab, to the extent of its ability and within the respective legal framework.

Prodhab does not currently count with a set budget. However, the budgetary issue is included in the legislation and shall be set pursuant to the necessary circumstances of its individual components.[103] In addition to the appropriate control on the allocation of resources, Prodhab shall be subject to compliance with the principles on Financial Management of the Republic and Public Budgets and shall provide any information required by the Ministry of Finance.[104] In addition, Prodhab shall be subject only to the provisions of the Comptroller General of the Republic

To date, the Constitutional Court has been responsible to resolve cases concerning privacy/personal data. Pursuant to statistics of the Costa Rican Legal Information System (SCIJ), the Court has received 1396 cases claiming violation of privacy and 266 cases claiming an violation on data protection.

iii. Remedies/Recourse:

An individual who believes his/her rights have been affected by the processing of his/her personal data must formally request that the data processor remove, update or block the information in question, or that it not be used for purposes other than those for which it was collected, pursuant

[101] Ley No. 8968, artículo 15
[102] Article 18
[103] Law No.8968, Article 20,
[104] Law No.8131,Titles II and X, September 18, 2001.

to the principles of informational self-determination contained in the data protection law. This procedure must be followed before resorting to an amparo suit to protect the individuals affected rights.

A person whose rights of privacy/data protection have been affected can bring a case before the proper jurisdictional court, pursuant to civil, criminal or administrative law. For civil liability against an offender - including any company that deals with personal data, and in in a situation not resolved by the Prodhab, the individual may sue for infringement of civil law, establishing the damages he/she has suffered. It should be noted that filing a lawsuit based on the aforementioned liability does not preclude a parallel or subsequent appeal under Costa Rican law to further protect the fundamental rights of the individual.

Also, if the petition presented with the data processor was not responded or if the individual was not satisfied with the response, he/she may go directly to the Constitutional Court and file an amparo appeal. The individual may also use this recourse to request that the data processor update, correct, block or remove his/her personal data.

iv. Investigatory Capabilities/Criminal Prosecution:

As discussed above, the enforcement procedure under the data protection law allows Prodhab the opportunity act on an ex-officio and ex parte basis. Generally, in cases where Prodhab sees an indication of violation of an individual's right to privacy/data protection, the Agency may initiate a procedure to analyze whether the data in possession of the processor is being processed in accordance with the principles and requirements of the law. In addition, whenever applicable and not contrary to the data protection law, the procedures set forth in the General Law of Public Administration will also apply for the regular procedure. Appeals to the resolutions of the Prodhab must be brought within three days.[105]

Under Costa Rican law, misuse of intimate or private data is considered a criminal offense, punished under the criminal code, which provides prison sentences from six months to two years for a person who infringes the privacy of another, or without consent takes possession, accesses, modifies, alters, deletes, intercepts, interferes, uses, broadcasts or diverts information from its destination, records data and images on electronic media, computer, magnetic and telematics. The penalty for the actions when performed by persons responsible for the electronic, computer, magnetic and telematics will range between one and three years.[106]

Complaints for these actions are handled by prosecutors for violation of an individuals communications, so long as the prima facie elements of a criminal case are present, that is, intent of the active subject to infringe the privacy of the victim or discover his/her secrets, or that the action was conducted without the authorization of the individual. Since 2001 when the penal sanction was enacted, the judiciary has received 169 cases alleging violations of electronic communications, according to the following statistical table:

[105] Law No. 8968, article 27
[106] Penal Code No.4573 of May 4, 1970, Article 196 bis

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	TOTAL
Violation of Electronic Communication	0	0	0	7	5	11	21	32	51	42	169

C. Cross-Border Cooperation

i. Data Transfer:

Pursuant to the data protection law, the general rule is that the data processor (whether public or private sector) may only transfer data when the individual has consented explicitly and validly to the transfer and such transfer was made without violating the principles and obligations under the law. This protection covers not both domestic and international transfers.[107]

ii. International Instruments/Arrangements:

Costa Rica is not party to any international instruments or arrangements on cross-border cooperation on privacy/access to information. However, Costa Rica is member of the Ibero-American Network on Data Protection and signed the Declaration of Antigua Guatemala, which establishes voluntary guidelines on privacy/data protection. Likewise, Costa Rica participated in the XIII Ibero-American Summit in 2003, in which the Heads of State declared that, aware that the protection of personal data is a fundamental right of people, stressed the importance of Latin American regulatory initiatives to protect privacy of citizens in the region. In other international forums, such as the Political Dialogue and Cooperation between the European Community and its Member States and the republics of Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Panama, in 2010, Costa Rica cooperated with the other states to ensure protection of personal data, improve the level of protection, and promote the free movement across borders.

Costa Rica has not yet requested certification from the European Union.

ii. Cross-Border investigatory and enforcement cooperation:

As a rule Costa Rica's legislation allows the exchange of information with authorities in jurisdictions outside the territory, especially in national and transnational organized crime such as terrorism, drug trafficking, bank fraud, etc.108 However, this can depend on the particular offense concerned. Given the still recent enactment of a law on personal data protection, and current process to establish a data protection agency, it seems unlikely that authorities, at least in the short term, will be in capacity to cooperate cross-borders on privacy/data protection. In addition, the data protection law does not expressly provide for cooperation with governments and data protection agencies, or obligations to Prodhab to cooperate with foreign data protection/enforcement agencies. It is possible, however, that such cooperation become commonplace in the future.

[107] Law No. 8968 of July 7, 2011, article 14
[108] Ley contra la Delincuencia Organizada No.8754 de 22 de julio de 2009, artículo 11

D. Case Law and Special Challenges

National case law has allowed citizens to exercise rights related to the treatment of personal data. However, courts have been presented with special challenges due to the existence of a new right without the benefit of specific legislative provisions on privacy/data protection. Cases were initially decided on grounds of on traditional concepts of privacy or intimacy, but led to confusing and even contradictory jurisprudence. The courts gradually came to recognize the right of informational self-determination and the protection of personal data, however, leading to more uniform criteria and application in the judicial system. Of particular importance, the Constitutional Court recognized the right of informational self-determination to contain the following principles, setting guidelines for subsequent cases: transparency on the type, size or purpose of the processing of stored data, the correspondence between ends and storage utilization and employment information, the accuracy, reliability, timeliness and full identification of the stored data, prohibiting the processing of data relating to the private sphere of citizens (race, religious beliefs, political affiliation, sexual preference, etc.) by non-expressly authorized to do so and anyway, use that information must be made in line with what it seeks, the destruction of personal data once it has been fulfilled the purpose for which they were collected, among others . Another important decision of the Constitutional Court establishes a certain hierarchy for types of personal data, according a higher level of scrutiny and security for sensitive data relating to sexual preference, ethnicity, religion and political affiliation, considered and inherent aspects of personality.[109]

5. Dominican Republic

A. Legal Context

i. Constitutional Framework:

The Dominican Constitution provides for the following rights: right to privacy and honor,[110] right of access to information and freedom of expression,[111] and writ of habeas data.[112]

[109] For a detailed discussion and history of Costa Rican case law on privacy/data proteccion, please see Costa Rica's response to Questionnaire on Privacy and Data Protection Legislation and Practices, contained in document CP/CAJP-3026/11 add. 6 available at the following webpage: http://www.oas.org/dil/esp/proteccion_de_datos_cuestionario_Costa_Rica.pdf

[110] Constitucion de la Republica Dominicana, Articlo 44.

[111] Article 49. - Freedom of expression and information. Everyone has the right to express his/her thoughts, ideas and opinions freely without censorship: 1) All persons have the right of access to information. This right includes search, seek, receive and it disseminate information of all kinds, in public character, by any medium, channel or media, pursuant to the constitution and the law; 2) All journalist media have free access to official and private sources of information in the public interest, in conformity with the law; 3) The secrecy and the journalist's consciousness clause are protected by the Constitution and the law; 4) All persons entitled to benefit of correction when injured or offended by disseminated information, pursuant to the law; 5) The law guarantees equal access to all social and political sectors.

[112] Constitution, Article 70. Everyone is entitled to a judicial action to deal with the existence and access to the data it contained in public or private records or databases and, if false or discriminatory, may require the suspension, modification, maintenance and confidentiality of those, according to law.

ii. Legislative Framework:

Article 44 of the Constitution provides a broad right to privacy and personal honor, establishing that all persons have the right to privacy -- non-interference with privacy, family, home and correspondence of the individual, as well as the right to honor, good name and reputation. Any authority or individual (public or private) that violates such right or is obliged to compensate the right-holder according to law.[113] in addition, the law in Dominican Republic does provide specific/sectoral rules on privacy/data protection in the following specialized contexts: Tax Code; Criminal Procedure Code; Code for the Protection of Children; the Criminal Code; the General Law on Access to Public Information; Regulation of credit information companies and protection to the holder of the information;[114] Monetary and Finance Code;[115] Law on Acquired Immune Deficiency Syndrome;[116] General Health Law;[117] Telecommunications Law;[118] and Regulations for Authorization of Telephone Interventions.[119]

At the present time, a Draft Law on Protection of Personal Data is under consideration by the Executive branch, prior to sending to the Congress for possible approval.

[113] Constitution Article 44: Specifically establishes that: 1) The home address and any private person shall be inviolable, except in cases that are ordered in accordance with the law, by competent judicial authority or in case of a flagrant crime; 2) Everyone has the right to access information and data to his or her assets, whether they are located in official or private records, and to know the destination and the use made of them, with the limitations set by the law. The processing of personal data and information assets must comply with the principles of quality, legality, loyalty, security and purpose and may apply to the competent judicial authority the update, oppose the processing, modification or destruction of information affecting those rights unlawfully; as well as 3) Tthe inviolability of correspondence, documents or physical formats private messages, digital, electronic or any other type. They may be accessed, intercepted or recorded, only by order of a competent judicial authority, by law and subject to due process; 4) The handling, use or processing of data and information from official authorities that collect the prevention, prosecution and punishment of crime, may only be processed or communicated to the public records, who was involved from an opening proceedings in accordance with the law

[114] Law Number 288-05

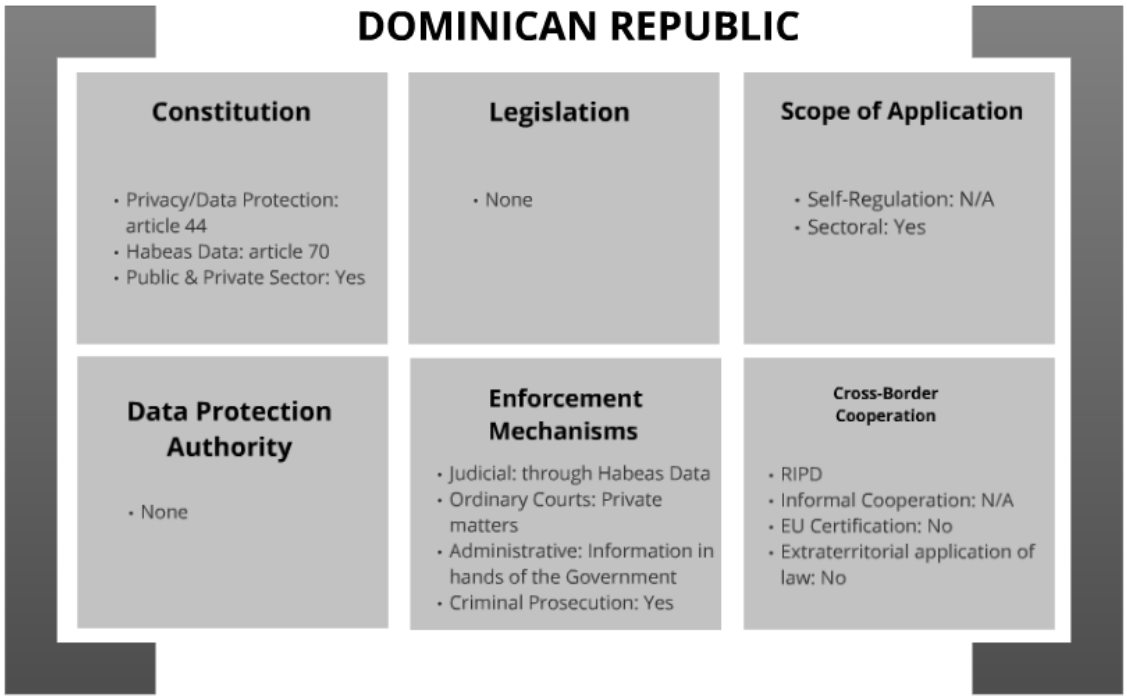
[115] Law Number 183-05

[116] Law Number 55-93

[117] law Number 42-01

[118] Law Number 153-98

[119] Law Number 122-07



iii. Habeas Data:

The Dominican constitution establishes the writ of Habeas Data.[120] Included in the Organic Law of the Constitutional Court and Constitutional Procedures, Habeas Data may be filed in any court of the republic under the amparo system. The specific procedure on habeas data establishes that all persons are entitled to a judicial action to know the existence of personal data, to access such data be it in public or private databases. In those cases in which the information is found to be incorrect or discriminatory, such individual may require the suspension, rectification, updating, and confidentiality thereof.[121]

iv. Self Regulation:

There are currently no self-regulatory codes of conduct on privacy/data protection in the Dominican Republic.

[120] Constitution, Article 70, which establishes that everyone is entitled to a judicial action to deal with the existence and access to the data contained in public or private databases. In cases where the information is false or discriminatory, the affected individual may require the suspension, modification, maintenance and confidentiality of the information

[121] Organic Law of the Constitutional Court and Constitutional Procedures, Article 64. The law further establishes that the action of habeas data is governed by the procedural amparo system

B. Enforcement

i. Enforcement Mechanisms:

At present, the only mechanism for the enforcement of privacy/personal data rights is the writ of Habeas Data (as described above). With regard to causes of action for information held by private parties, the action should be brought before the ordinary courts. With regard to causes of action for information held by State agencies, the action should be brought under administrative jurisdiction.[122]

ii. Data Protection/Enforcement Authorities:

The Dominican Republic does not count with an organ responsible for comprehensive compliance with privacy/data protection. There are, however, government agencies with oversight functions under some local laws and regulations that touch upon the subject. One example is deal with the protection of consumer rights in general (which can include privacy rights), oversight functions fall on Dominican Institute for Protection of Consumer Rights (Proconsumidor) and justices of the peace of the Dominican Republic.[123] In the case of data in processed by private credit bureaus, oversight functions fall within the duties of the Superintendency of Banks.[124]

iii. Remedies/Recourse:

Affected individuals must seek enforcement via the writ of Habeas Data. The Attorney General may also pursue actions against public or private actors for violation of privacy rights under the Code of Criminal Procedure.

C. Cross-Border Cooperation

i. Data Transfer:

Local law does not condition the cross-border flows of information.

ii. International Instruments/Arrangements:

Dominican Republic has participated in the Ibero-American Network on Data Protection but is not party to any formal agreements or arrangements on cross-border cooperation.

iii. Cross-Border investigatory and enforcement cooperation:

The Dominican Code of Criminal Procedure allows information exchanges with foreign authorities and courts concerning in cases under investigation.

---

[122] Law no. 13-07
[123] Constitution and Law Number 358-05
[124] Law no. 288-05

D. Case Law and Special Challenges

Pursuant to information provided in the Dominican Republic's answer to the Questionnaire on Data Protection, the local courts have received only one case touching upon privacy/data protection.

6. El Salvador:

A. Legal Context

i. Constitutional Framework:

Constitutionally there is no explicit regulation on the protection of privacy/data protection in El Salvador. However, Article 2 of the Constitution guarantees the right to honor, personal and family privacy and the right to one's own image. As a result, in El Salvador the right to information self-determination has been derived as a fundamental right implicitly incorporated in the Constitution.[125] Although the rights to privacy/data protection are not covered by the Constitution expressly, they can perfectly fit within article 2, as they have a close relationship with personal and family intimacy/privacy and self-image, so that their care would not be excluded from the rights recognized in the Constitution.

The Constitution also makes express reference to freedom of expression, recognized in Article 6, which establishes that: "Every person may freely express and disseminate their thoughts whenever they do not disturb public order or morals, honor, or the private life of other persons."

The writ of Habeas Data is not included in the Constitution of El Salvador.

ii. Legislative Framework:

El Salvador does not have a law that governs privacy/data protection in a systematic manner. However, the local legal framework does count with a number of existing laws which touch on essential aspects of privacy/data protection. Other secondary legislation has also incorporated provisions relating to privacy/data protection into its regulatory system, most of which are applicable equally to public sector and private sector contexts.

Some of these laws include: the Penal Code, which governs violation to persons honor and privacy (Articles 177 to 190),[126] the Code of Criminal Procedure, Ethics in Government Act, Consumer Protection Act,[127] Banks Act, especially with regard to banking secrecy;[128] Anti-Money Laundering and Assets Act;[129] Special Law for the Protection of Victims and Witnesses; Central American Convention for the Protection of Victims, Witnesses, Experts and other Persons

[125] The right to data protection and privacy is understood implicitly contained in the Art.2 of the Constitution which states establishes that all persons have the right to life, physical and moral integrity, to freedom, safety, labor, property and possession, and to be protected in the conservation and protection of personal honor, personal and family privacy and personal image.
[126] Penal Code, Articles 177 to 190.
[127] Consumer Protection Act, Article 49.
[128] Banks Act, Article .232.
[129] Anti-Money Laundering and Assets Act, Articles 24 and 25

involved in the Investigation and the Criminal Process, particularly drug trafficking and organized crime; procurement Act of the Public Administration; the Access to Information Law, already in enacted but in the process of its effective implementation, which prohibits providing information or records considered confidential personal character;[130] the Juvenile Criminal Law which recognizes the right to personal privacy of minors and which regulates confidentiality of the Record Book;[131] the Law on Protection of Children and Adolescents, which recognizes the rights to honor, image, and privacy, among others.[132]

iii. Habeas Data:

The Salvadoran legal system does not provide a figure of habeas data. However, this does not mean that such right is unprotected. As mentioned, Article 2 of the Constitution includes this right implicitly, and Section 247 of its regulatory law establishes that: "Every person can seek protection before the Constitutional Chamber of the Supreme Court for violation of the rights granted by this Constitution," which is understood to mean that rights expressly and implicitly contained must be guaranteed to every person through the protective mechanisms and recourse.

iv. Self Regulation:

In El Salvador there are no regulations specifically governing the privacy/data protection. As a result, there are no self-control codes or other similar self-regulation systems for the protection of

[130] Access to Information Law, Arts.24, 31 - 44.
[131] Juvenile Criminal Law, Article 5 and Article 122 and 123
[132] Law on Protection of Children and Adolescents Art. 46.

those rights. In any case, within the Salvadoran legal system, there are a few scattered rules related to this aspect, such as the Code of Journalistic Ethics.

B. Enforcement

i. Enforcement Mechanisms:

The Salvadorian Constitution establishes that "any person may seek protection before the Constitutional Chamber of the Supreme Court for violation of the rights granted in the Constitution." It includes express and implied rights, which must guaranteed to every person through the protection mechanisms established.[133] So, even in the absence of specific legislation it can be understood that privacy/data protection can be secured through the process of constitutional process.

Within the criminal sphere, honor and privacy are understood as legal goods worthy of protection. Therefore, El Salvador has criminalized a set of behaviors that pose a serious injury to these goods. For example, the code of criminal procedure indicates that such crimes are prosecuted by private action -- accusation by the victim.[134] Furthermore, this law regulates a special (and more expedited) procedure that can also be used in these cases.[135]

ii. Data Protection/Enforcement Authorities:

Since El Salvador does not have a data protection law, it also does not have a data protection authority. As a result, the authorities whose primary responsibility of it is to uphold the current laws related to privacy/data protection laws are judges of the Constitutional Chamber of Supreme Court, who may hear specific case brought via the amparo process.

iii. Remedies/Recourse:

As mentioned, remedies available to the individual the privacy/data protection rights of whom have been violated would center on the amparo process and the criminal code for prosecution of crimes against the aforementioned rights.

iv. Investigatory Capabilities:

There are no investigatory capabilities of the authorities, except in discovery during cases brought before the judiciary.

---

[133] Constitución Art.247

[134] Code of Criminal Procedure, Art.28

[135] Code of Criminal Procedure, Arts. 439 to 444. An expedited procedure for enforcement of privacy rights include: a) presentation of the indictment before a court of judgment; b) summons of the accused; c) conciliation; d) hearing input and admission of evidence, and e) judgment.

C. Cross-Border Cooperation

El Salvador in not party to any international agreements on privacy/data protection. The transfer of data is not regulated or prohibited under the current legal framework. International cooperation is possible under international criminal cooperation process and under local law.

7. Mexico:

Mexico provided a response to the CJPA's Questionnaire on Privacy and Data Protection Legislation and Practices, via verbal note number OEA-00265, dated February 8, 2012. This response is contained in document CP/CAJP-3026/11 add. 7 and provides the foundation for the information summarized in the present section.

A. Legal Context

i. Constitutional Framewok:

The Political Constitution for the United Mexican States has several provisions related to privacy/data protection. Article 6 refers to freedom of expression, access to information and data protection, establishing that the manifestation of ideas can not be subject to judicial or administrative inquiry or limitation, unless it is against morality, the rights of third parties, produces the commission of a crime, or disturbs the public order. It also establishes that the right to information must be guaranteed by the State and that the federal and state governments must protect all information having to do with a person's privacy and personal data – subject to exceptions provided by law.

Article 7 establishes the right of freedom of expression, guarantees freedom of the press, and guarantees that no government authority may censor or violate freedom of writing and publishing on any subject. The one limitation to this right has to do when dealing with the private lives of individuals, as well as public morals and public peace.

Article 6 also grants individuals the habeas data right to have free access to their personal data in the hands of public entities, and to rectify/correct such should it be incorrect. Article 16 further establishes that all persons are entitled to the protection of their personal data, that all persons have the right to access, correct and remove their personal data, as well as the right to express their opposition to its processing pursuant to law, which shall establish exceptions for processing personal data for reasons of national security, public order, public health, safety, and to protect the rights of others.

Article 20 establishes rights to withhold and/or access personal data for individuals to defend themselves in criminal proceedings and Article 73 (section XXIX-O) grants the Federal Congress the power to legislate on personal data in possession of private persons/entities.

ii. Legislative Framework:

At the national level, Mexican legislation on privacy/data protection covers the public and private sector. Federal legislation on transparency/access to information regulates data protection when dealing with information processed by or in custody of federal government agencies. The federal Law for the Protection of Personal Data in the hands of the Private Sector ("FLPPD") regulates

privacy/data protection for information processed by or in custody of private individuals/entities on a nation-wide basis. At the State level, the thirty one states (and the federal district) have enacted transparency/access to information legislation, which also regulate data protection for information processed by or in custody of state government agencies. State legislation does not apply to the private sector, which is regulated nationally by the FLPPD.

Public Sector: At the national level, legislation which regulates privacy/data protection in the public sector includes: 1) the Federal Law on Transparency and Access to Public Information; 2) the Regulation to the Law on Transparency; and the 3) Federal Guidelines for Personal Data Protection.

The Mexican (Federal) Law on Transparency and Access to Public Information, and its regulation, establishes a framework for protection of personal data in possession of public authorities (regulated entities). This law establishes the governing principles, including when personal data can be processed, collected and used, requires the consent of the individual whose data is being collected and/or processed (with exceptions), and requires that collection and processing must be for a specific purpose. The law creates a right to access and correct the information, establishes duties of confidentiality and security, and establishes an independent federal authority to ensure compliance.[136]

The Regulation to the Transparency Law establishes the procedure by which individuals can request access to his/her personal data before all federal agencies and to request correction if the information is incomplete and/or incorrect. The regulation also establishes an appeal procedure

[136] Mexican (Federal) Law on Transparency and Access to Public Information, Titulo I, Capitulo IV ("Proteccion de datos personates") y Titulo II, Capitulo IV ("Del procedimiento ante el IFAI").

before the Federal Institute for Access to Information for cases in which the individual is not satisfied with the resolution of the issue by the federal agencies.[137]

The Federal Guidelines for Personal Data Protection establish binding policies and procedures for agencies of the Federal Civil Service to ensure that individuals have the right to decide regarding the use and destination of their personal information, to ensure that it is processed and handled properly, and to prevent its unlawful and/or harmful transmission.[138] The Guidelines also establish principles that govern processing of personal data by the federal public administration and establish conditions and minimum requirements for its handling and safekeeping.

At the level of the thirty one states (and the federal district), states have enacted laws on transparency/access to information which also regulate data protection for information processed by and/or in custody of the agencies of the local state government. Table ___ provides the list of the applicable state laws on transparency/access to information.

Private Sector: At the national level, the legislation which regulates privacy/data protection in the private sector is the Federal Law for the Protection of Personal Data in the hands of the Private Sector (FLPPD) and its Regulation.

The FLPPD, published on July 5, 2010, aims to protect personal data to ensure it is processed for legitimate purposed based on informed consent, to ensure the right of privacy and of self-determination of all individuals. The law applies to all persons (individuals and legal entities) who collect, obtain, process, use, disclose and/or store personal information.[139] It excludes credit information agencies and persons who collect information for purely personal or domestic purposes.[140]

The regulation to the FLPPD establishes the framework for the effective application of the law, including: its territorial scope of application; source for public access to individual's private data; specific characteristics of consent; procedure to obtain compensatory measures; specific duties and obligation of the data processor and subcontractors/third party processors; procedures for binding self-regulation; verification procedure; and the procedure for the protection of the individual's rights. As mentioned, the FLPPD applies to all private sector parties in the entire country.

iii. Habeas Data:

As discussed in subsection (i) above, Article 16 of the Mexican Constitution establishes an individual's right to access his/her personal information, as well as the right to rectify, to cancel and to oppose the use and/or processing of personal data (ARCO rights). These rights are implemented via specific laws for public and private sectors persons/entities who process and/or collect personal data.

Regarding personal data in possession of the federal government, the Federal Law of

---

[137] Capttulos VI ("Informacion confidencial"), VIII ("Proteccion de datos personales") y XII ("Del procedimiento de acceso a la inforrnaciOn", con algunas disposiciones aplicables al acceso y rectificacion de datos).
[138] Federal Guidelin on Data Protection Number 1.
[139] Articulo 1 de la LFPDPPP.
[140] Articulos 2 y 3, fracciOn XVIII de la LFPDPPP.

Transparency and Access to Public Information and its Regulation establish the specific process to access and correct personal data in custody or possession of federal agency.

Regarding personal data in possession of the state government, each Mexican state has its own legal instrument that guarantees the right of access to personal data in possession of the public entities of the state in question.

Regarding personal data in possession of the private sector, the FLPPD regulates access to personal data in possession of private parties (individuals or legal entities). In contrast to the bifurcated system for access to personal data in hands of the public sector, the Federal Law on Data Protection regulates access to personal data in hands of the private sector at both federal and state level in the entire country. Specifically, the LFPPD guarantees that the individual has the right to access his/her personal information, has the right to rectify it, cancel it and to oppose the processing thereof. Article 22 of the LFPDPPP provides that:

> Any owner of personal data may exercise the rights of access, rectification, cancellation and opposition under this law. Exercise of any of these rights is not a prerequisite for, nor prevents the exercise of another. Personal data must be safeguarded in such a manner as to permit the exercise these rights without any delay thereto.

Article 23 of the FLPPD further provides that the individual is entitled to access his/her personal data held by the controller, as well the right to access the privacy policy to which the data is subject. Article 24 provides that the individual is entitled to correct the data when it is inaccurate and/or incomplete. Article 25 provides that the individual has the right, at all times, to cancel (delete) his/her personal data. And Article 27 provides that the individual shall be entitled at all times to oppose the processing of his/her personal data for legitimate reasons.

iv. Self Regulation:

Recognizing that individuals and entities have the right to agree among themselves to the terms and conditions for the processing of personal data, the FLPPD provides for the creation of self-regulatory schemes, which shall be binding on the parties.[141] All self-regulatory schemes must be reported and registered before the Federal Institute for Access to Information and Data Protection (IFAI) to be effective.[142]

As of march 2012, the registry for self-regulatory schemes has not been fully instrumented; thus self-regulatory schemes have not yet been presented for registration with IFAI. However, there are private companies that do have existing self-regulatory schemes that incorporate provisions on privacy/ data protection, including the following three examples.

The Mexican Internet Association--a private institution that brings together companies in the Internet industry in Mexico--provides an *electronic seal* that recognizes businesses or institutions comply with its information and privacy procedures. A company that receives the seal agrees to

[141] FLPPD Article 44
[142] Regulation to the FLPPD, Article 86

comply with the MIA's privacy rules and code of ethics.[143] The Seal requires compliance with minimum standards, including the creation of a privacy policy, disclosure notices, options and consent, data quality and limitations of use and safety. This Code of Ethics also establishes penalties for any member who fails to comply with this standard.[144]

The BBVA Financial Group has a established a code of ethics, including provisions on privacy/data protection for all its affiliates, which provides specific rules and procedures to protect and ensure proper treatment of information of a personal character obtained from their business operations and which is related to their customers, shareholders, employees and managers, or any other person with whom they interact. The Code provides, inter alia, the following responsibilities to the institution and its employees: the right to access internal rules and procedures for information security and protection of personal data; the right to apply appropriate measures to prevent improper access to such information; the obligation that employees who, by reason of their job functions, have access to personal data are deemed responsible for the safekeeping and proper use of such data.

The Novartis Group, comprised of companies that develop pharmaceutical products, has also created a code of ethics which includes the privacy rights of its employees, patients, physicians and other interest groups. The code requires that individuals be notified regarding the collection and processing of their personal data, that such collect and processing take place only for legitimate and specific business purposes, and the obligation to protect such data from breach and unauthorized access.

These represent some examples of current self-regulation in Mexico, clarifying that the schemes and policies described therein have not been filed, registered and/or approved by IFAI, and that IFAI has not participated in any way in the creation and review of the same. Once the system for the filing of self-regulation schemes is complete, IFAI will assist those entities interested in establishing their binding self-regulatory schemes and will provide oversight to ensure compliance therewith.

B. Enforcement

i. Enforcement Mechanisms:

Enforcement mechanisms in Mexico can be voluntary and compulsory. With regard to mechanisms for voluntary compliance, the FLPPD allows the parties to agree among themselves (or with civilian and governmental organizations, at the national or foreign level) on binding self-regulation schemes, which may take the form of codes of ethics, professional best practices, trust-marks or seals, privacy policies, corporate privacy policies, or any other form reported and registered before IFAI and other competent sectoral authorities.[145]

The minimum standards/content for these self-regulatory schemes are provided for in the FLPPD and include the following: scope of application, compliance procedures to meet and measure

---

[143] In particular, the seal of the MIA promotes compliance with the FLPPD and its Regulation, the Federal Law on Consumer Protection, the MIA Code of Ethics, and the Privacy Framework of the Asia Pacific Economic Cooperation. www.ampici.org.mx. www.sellosdeconfianza.org.mx.
[144] Article 22 MIA Code of Ethics.
[145] Articulo 44 de la LFPDPPP y 80 del Reglamento de la LFPDPPP.

compliance with personal data protection obligations, internal and external systems for supervision and monitoring, training programs for employees and individuals who to handle personal data, mechanisms to facilitate the rights of individuals, identification of all individual right-holders and persons who come in contact with the processed information, and enforcement procedures and corrective action in case of non-compliance.[146]

These self-regulatory schemes include the certification of those responsible for the protection of personal data, which may be awarded under a procedure performed by an accredited person/entity that guarantees that the privacy policies, programs and procedures implemented by the obligated party ensure the proper treatment of the personal data, and that the safety measures adopted by the person/entity are adequate to protect the information.[147] The FLPPD also provides for other non-coercive enforcement mechanisms by IFAI, including assisting other institutions in the development of their regulations, issuing opinions and recommendations, disclosing international standards and best practices, cooperation with national and international supervision authorities, conducting studies and investigations, and providing training to obligated entities.[148]

In terms of compulsory mechanisms, the FLPPD and its Regulations establish binding procedures for exercising the rights of access, correction, cancellation and deletion of personal data; procedures for the protection of the rights of individuals whose information in processed; procedures to verify compliance with the law and regulation; and procedures for imposing sanctions in cases of violation and non-compliance.

With respect to personal data in possession of federal government agencies, the procedure to access and correct takes place before the federal agency in question, via a request for access and data correction. If the applicant is not satisfied with the resolution of the matter, he/she may present an inconformity with IFAI, which will review and resolve on the issue. Although no cases have been brought yet under the Mexican law and regulation, it is possible that IFAI resolutions may be challenged before the Judicial Power of the Federation through the *amparo* action under Mexican law.

With respect to personal data in possession of state government agencies, state laws generally provide an administrative action, usually in the form of application, to exercise one or more of the following rights: access, rectification, cancellation and opposition; as well as an administrative appeal procedure to challenge unsatisfactory responses to the title- holders. This legal remedy is generally known as a 'complaint,' but depending on the legislation in question may be referred as a complaint, appeal for review, reconsideration, grievance procedure, etc.

For both public and private sector cases, the court systems provide a final recourse when individuals are not satisfied with the resolutions of the other levels.[149]

ii. Data Protection/Enforcement Authorities:

With regard to privacy/data protection in the context of the private sector and the agencies of the federal government, the Data Protection Authority is the Federal Institute for Access to

[146] FLPPD Regulation article 82.
[147] FLPPD Regulation Articulos 83 y 84.
[148] FLPPD article 39
[149] Actions for the protection of personal data in the courts would occur via amparo the "Law on Amparo, Regulatory Rules 103 and 107 of the Mexican Constitution.

Information and Data Protection. The Institute is a decentralized agency of the federal government, with operational, budgetary and decision autonomy, in charge of promoting and disseminating the right to information, to decide on the denial of requests for access to information and protection of personal data processed or in custody of federal agencies.[150] In addition, IFAI is tasked with the dissemination of the right to privacy/data protection in Mexican society, with promotion of this right, and with monitoring compliance and enforcement with the Federal Law on Privacy and Protection of Data.[151]

For the year 2012 IFAI counts with a total of 393 employees and a total budget of MX$482,382,497 (Four hundred and eighty two million, three hundred eighty-two thousand four hundred ninety-seven Mexican pesos).[152]

In addition to IFAI, it should be noted that the following government authorities at the federal level are responsible for the implementation of their own rules on privacy/data protection: the Federal Legislature, the Judiciary of the Federation, the Universidad Nacional Autonoma de Mexico, the Banco de Mexico, the Federal Electoral Institute, the National Institute of Statistics and Geography, and the National Human Rights Commission.

With regard to privacy/data protection in the context state government agencies and the federal district, each state government has its own competent authority. These are divided into three groups: state access to information/data protection authorities with constitutional autonomy;[153] state access to information/data protection authorities with legal autonomy;[154] and state access to information/data protection authorities without autonomy.[155]

For the processing of personal data held by individuals, The LFPDPPP provides for the existence of two procedures related to compliance with the principles and rights of privacy. On the one hand in the LFPDPPP in its articles 45 to 58 establishes the procedure for protection of rights which in all cases is initiated at the request of the data subject or his legal representative, and also provides for in Articles 59 and 60 of the Procedure verification can start officio or upon request. In the verification procedure IFAI office has the authority to start where it suspects founded and substantiated the existence of violations of LFPDPPP.

iii. Remedies/Recourse:

IFAI is the administrative authority empowered to ensure compliance with the FLDDP and the FLTATI, both at its own initiative/prerogative it there is reason to believe a violation has occurred, as well in response to petitions made by individuals. IFAI can also hear appeals in cases where public authorities have refused to deliver or correct personal information, as well as in cases where the petitioner received no response. In the latter case, IFAI must reviews all

[150] In accordance with Article 33 of the LFTAIPG
[151] LFPPD Article 38
[152] www.apartados.hacienda.gob.mx/presupuesto/temas/pef/2012/temas/tomos/06/r06_hhe_afpefe.pdf. Budget and personnel figures cover all powers of IFAI, including its duties regarding the right of access to information and the right of privacy/data protection.
[153] Baja California, Campeche, Coahuila, Chihuahua, Durango, Estado de Mexico, Jalisco, Morelos, Michoacan, Puebla, Queretaro, San Luis Potosi, Tabasco and Tlaxcala.
[154] Aguascalientes, Baja California Sur, Colima, Chiapas, Distrito Federal, Guanajuato, Guerrero, Hidalgo, Nayarit, Oaxaca, and Quintana Roo.
[155] Sonora.

appeals brought before it, so long as they contain all necessary legal elements for consideration. Review is mandatory -- not voluntary or optional on a case-by-case basis.

With regard to the private sector, IFAI has the power to hear cases and to impose sanction against violators.[156] A second level of appeals is available to individuals, who may present recourse against IFAI resolutions before the Federal Court of Fiscal and Administrative Justice. And, as a third level, individuals may present an appeal against said court via a writ of *amparo* before the federal judiciary.[157]

In the case of the private sector, IFAI has received a total of 70 complaints against the private sector since it entry into force in January 2012.[158]

With regard to the public sector, IFAI has the power to hear and decide appeals in terms of both access to information and data protection. However, IFAI only has power to notify the federal agencies under its jurisdiction when a violation to the law and/or regulation was occurred; under the FLATI it does not have power to impose sanctions on public sector agencies. Unlike appeals against the private sector, it is also important to note that individuals have only one level of recourse against IFAI resolutions -- an *amparo* proceeding in the federal courts. Federal agencies, on the other hand, have no right to appeal. In their case, IFAI resolutions are final.[159]

In the case of the public sector (during the period of June 12, 2003 to December 31, 2011), IFAI received a total of 4,505 appeals on personal data. Of these, 4,373 arose from refusals by federal agencies to permit access to personal data in their possession. The other 132 resources arose from complaints related to the rectification of the information. During this period, IFAI has also received 11 complaints alleging improper processing of personal data by the public sector.

iv. Investigatory Capabilities/Criminal Prosecution:

The FLPPD provides two procedures for compliance: one initiated at the request of the data subject;[160] the other, a verification procedure, which can be initiated upon request of the title-holder or by IFAI where there is reason to suspect the existence of violations or upon request.[161]

IFAI also has power to conduct investigations and make recommendations on the protection of personal data pursuant to the Federal Law on Transparency and Access to Information.[162] In addition, binding self-regulatory schemes require certification by IFAI, which may conduct "proactive audits" at anytime before or after granting such certification. For this purpose, certification authorities will be accredited for this purpose and will conduct such certification in accordance with the parameters are established for such purposes.[163]

---

[156] the LFPDPPP in article 39, section VI,
[157] Article 56 of the LFPDPP
[158] The LFPPD was published in the Official Gazette of the Federation on July 5, 2010, but the exercise of rights of access, rectification, cancellation and opposition under the Law stems from January 6, 2012 under the Regulation.
[159] LFTAIPG in its article 37, section II
[160] articles 45 to 58
[161] Articles 59 and 60
[162] Articles 37, sections IX and XIX of the LFATIPG, 2, section V and 6 of the Regulations, as well as based on the forty-third of the Guidelines for the Protection of Personal Data.
[163] (art. 83 and 84 of the Rules of this Act)

Under the Mexican law, the authorities have parallel and proprietary investigatory authority and violations of the law can result in criminal prosecution. For the processing of personal data held by individuals, the federal law establishes illicit behavior which may lead to criminal liability.[164]

Complaints regarding illegal commercial gain from personal data may also be reported to the attorney general's office (ministerio publico), which is the administrative body responsible for carrying out investigations and prosecuting criminal matters. The entities responsible for privacy enforcement, on one hand, and entities responsible for criminal prosecution, on the other, are linked by the need for cooperation to determine the existence of possible criminal behavior, and to determine whether or not such behavior should be prosecuted before the courts.

C. Cross-Border Cooperation

i. Data Transfer:

Mexican law limits the domestic or international transfer of personal data, generally requiring that the receiving jurisdiction be subject to the same principles and rights that govern the processing of personal data under the FLPDD, in particular the need to observe the principles of notice and consent.[165]

In the case of domestic transfers, the Regulation requires that the recipient of the personal data become an obligated party under the law, subject to and covered by the law and regulations, and shall treat personal data pursuant to the terms and conditions agreed to under the privacy policy agreed to by the individual and the transferor.[166]

In the case of international transfers, Mexican law requires that these will only be possible when the recipient of the personal data assumes the same obligations that correspond to transferor.[167]

ii. International Instruments/Arrangements:

Mexican Law gives power to IFAI to cooperate with other national and international data protection and enforcement authorities.[168]

Although Mexico is not party to any instrument or arrangement related to international principles of privacy and cross-border flows of information, IFAI is committed to the protection of privacy and its principles across-borders and participates actively in the work on privacy/data protection, cross-border flows of information and cross-border cooperation currently taking place in the Organization of for Economic Cooperation and Development (OECD), Asia Pacific Economic Cooperation Forum (APEC) and the Council of Europe (CoE).

To highlight the importance of international instruments in Mexican law and practice, however, it should be noted that the OECD Privacy Guidelines and Trans-border Data Flow and the APEC

[164] LFPPD, Articles 67 and 68.
[165] Articles 36 and 37 of the LFPDPPP
[166] Regulation Articles 71 to 73
[167] Article 74 of Regulation LFPDPPP
[168] LFPDPPP (Article 39, fraction VII)

Privacy Framework are both taken into account in the drafting of the FLDDP. Mexico also participates actively in OECD's Working Party on Information Security and Privacy, belongs to APEC's Privacy Subgroup and part of the Executive Group on Electronic Commerce, is an observer of the Council of Europe and was accepted by the Committee of Ministers the Consultative Committee on the Modernization of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Mexico is also member of the Ibero-American Data Protection Network since 2003 and since 2010 IFAI President Commissioner Jacqueline Peschard has also served as President of that Network.

Mexico also has not received a privacy/data protection certification by the European Union. However, one of IFAI's goals in the international area is to promote and support concerned national authorities with the initiation of proceedings for certification by the European Commission. In this regard, the Mexican Ministry of Foreign Affairs, in charge of requesting the adequacy process, in also collaborating in the endeavor.

iii. Investigatory and Enforcement Cooperation:

Generally speaking, the Mexican legal framework gives the authorities of the various entities of government the power to implement mechanisms for communication and exchange of information with counterparts in other countries. In criminal matters, for example, the Ministry of Public Security and the Attorney General's Office (PGR) in accordance the Organic Law of the PGR, are authorized to exchange various information with their counterparts abroad.[169] Likewise, in administrative matters, local law allows the Federal Consumer Protection agency,[170] and the Ministry of Finance and Public Credit to exchange information with foreign governments.[171]

With regard to formal Cooperation via international arrangements such as the Global Privacy Enforcement Network (GPEN), APEC's Cross Border Privacy Enforcement Arrangement, or the Ibero-American Network of Data Protection, Mexico is not formally part of GPEN or the APEC Arrangement. However, the Mexican Government and IFAI participate in meetings of both mechanisms. Moreover, the IFAI has been one of the main drivers of the work of the Ibero-American Network on Data Protection from its creation and IFAI currently functions as president of the said network.

D. Case-Law and Special Challenges

Case law in Mexico, at the federal level, as well as at the level of the resolutions of IFAI, provide certainty in relation to the interpretation and scope the Federal Judicial Branch gives certain legal precepts including in the protection of personal privacy.

There are also several significant challenges to the implementation of the laws on privacy/data protection in the fields of communications, electronic banking and child protection, to name a

[169] Ministry of Public Security internal rules, Article 26, available at www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/770061/archivo; and Organic Law of the PGR, Article 5, available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LOPGR.pdf.
[170] Article 24 of the Federal Law of Consumer Protection.
[171] Articles 15 A and 36 B of the Bylaws of the SHCP

few.

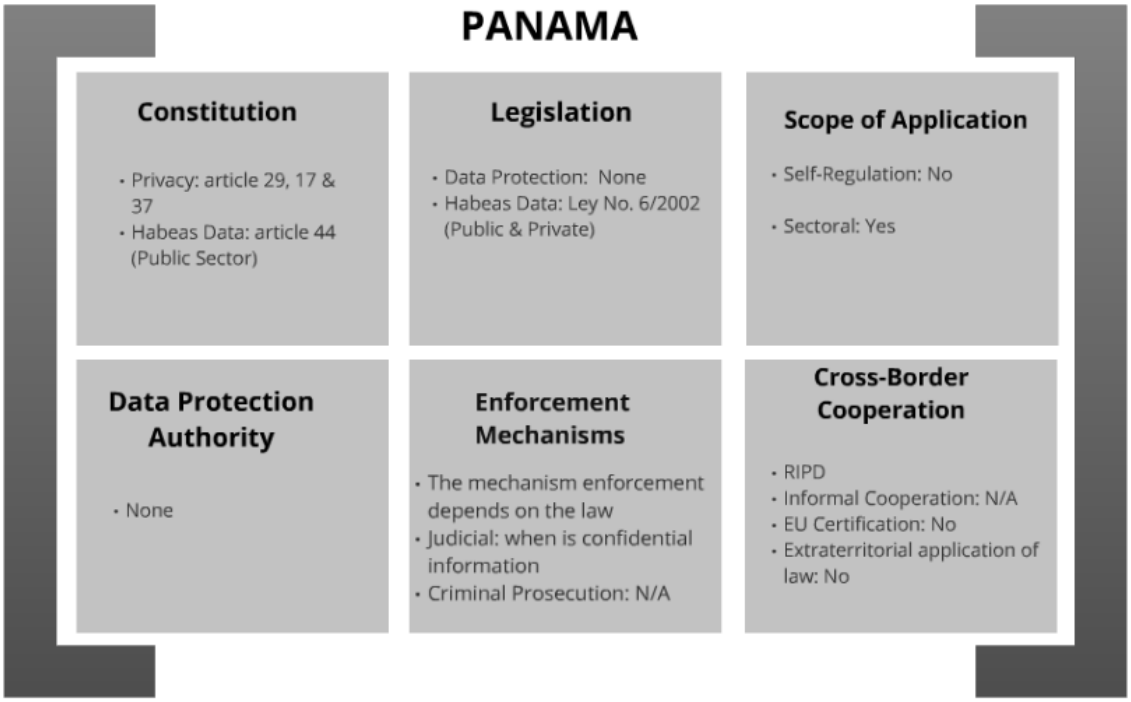
The regulation of social networks also presents special challenges, both for the breadth of users, on one hand, and the difficulty of applying local law to companies established outside Mexican territory. These challenges include issues of jurisdiction and choice of law, cloud computing, and require the existence of a legislative design sufficient to generate criteria for the application of national laws to the phenomenon of dematerialization produced by the internet and developments related thereto.

Additionally, the regulation of Cloud Computing involves major challenges in the following areas: security administration by service providers; protection of the rights of individuals; security architecture; monitoring and administration of security incidents and breaches; testing and safety measures; training of staff; transparency; control options for the user; portability and use of personal data; interoperability; data protection and compliance; certification; and providers of services to the public administration.

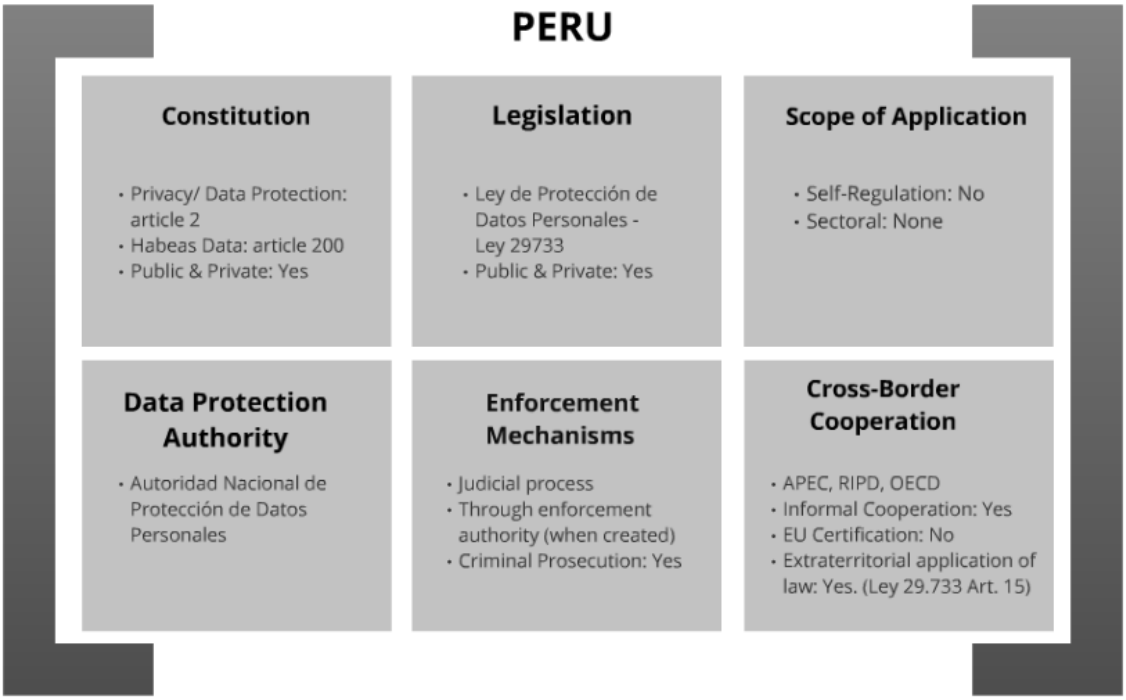
The regulation of telemarketing via SMS, e-mail, MMS, pre-recorded telephone calls and faxes, among others, also provides great challenges for the regulation of electronic communications. The same is true for in cases in which companies use data collected automatically via the Internet or through newsgroups, forums, mailing lists and data on the Internet.

Finally, a topic of particular interest deals with video surveillance, which involves two legal interests of major relevance for Mexico: security and privacy/data protection. In this case the challenge is to achieve a balance that properly accounts for the scope and importance of each.

8. Panama:


PANAMA
Constitution
• Privacy: article 29, 17 & 37
• Habeas Data: article 44 (Public Sector)
Legislation
• Data Protection: None
• Habeas Data: Ley No. 6/2002 (Public & Private)
Scope of Application
• Self-Regulation: No
• Sectoral: Yes
Data Protection Authority
• None
Enforcement Mechanisms
• The mechanism enforcement depends on the law
• Judicial: when is confidential information
• Criminal Prosecution: N/A
Cross-Border Cooperation
• RIPD
• Informal Cooperation: N/A
• EU Certification: No
• Extraterritorial application of law: No

9. Peru:



10. United States

The United States provided a response to the CJPA's Questionnaire on Privacy and Data Protection Legislation and Practices in document CP/CAJP-3026/11 add. 9 and provides the foundation for the information summarized in the present section.

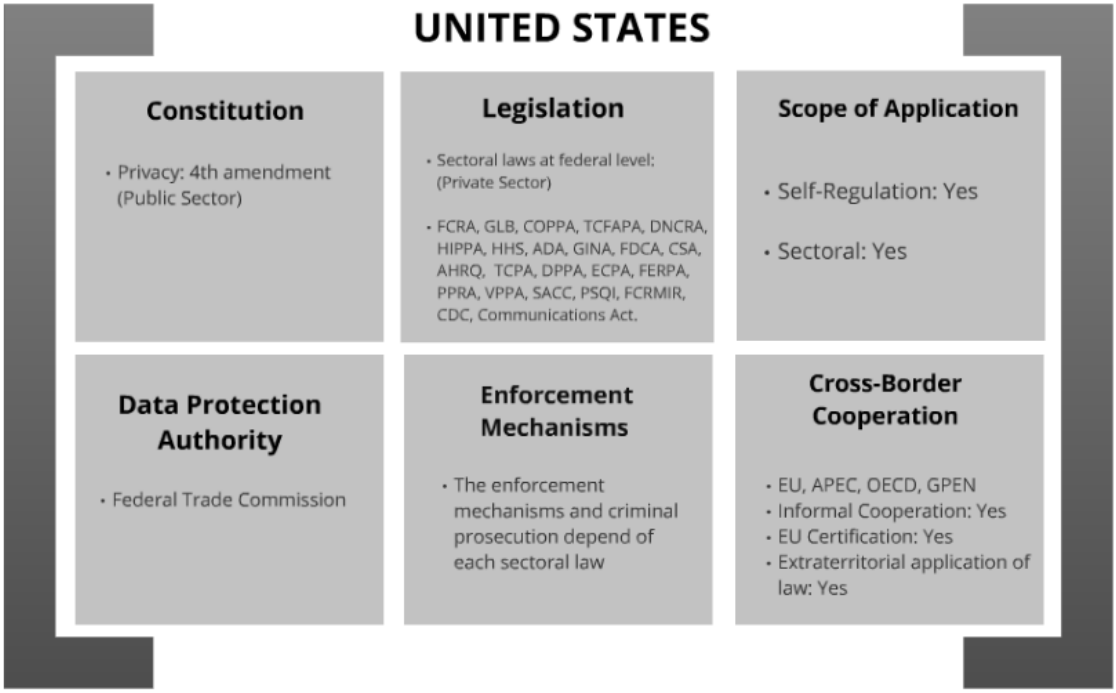
A. Legal Context

i. Constitutional Framework:

The Fourth Amendment of the U.S. Constitution protects freedom from arbitrary and unlawful interference with privacy. The Fourth Amendment, with certain exceptions, prohibits the government from conducting unreasonable searches and seizures. Government searches and seizures 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.[172]

[172] See National Conference of State Legislatures listing at http://www.ncsl.org/issues-research/telecommunications-information-technology/privacy-protections-in-state-constitutions.aspx.



ii. Legislative Framework:

FEDERAL LEGISLATION: At the federal level, the United States has enacted a number of sectoral laws.[173] Several fall within the authority of the U.S. Federal Trade Commission (FTC), which has broad authority in the commercial privacy area and oversees enforcement under the following laws:[174]

---

[173]. The information provided focuses on secotral laws those implicating the private or commercial sector rather than governmental use of personal data. 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.

[174]. 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.

Federal Trade Commission Act:[175] 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, monetary remedies in the form of consumer redress and disgorgement of ill-gotten gains, and other appropriate equitable relief.[176]

Fair Credit Reporting Act: [177] 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.

Gramm-Leach-Bliley Act:[178] Title V, subtitle A, of the Gramm-Leach-Bliley 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)[179] 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.

---

[175] 15 U.S.C. § 41 et. seq.
[176] 15 U.S.C. § 53(b).
[177] 15 U.S.C. § 1681 et seq. as amended, available at http://www.ftc.gov/os/statutes/031224fcra.pdf.
[178] 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.
[179] 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.

Children's Online Privacy Protection Act:[180] 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,[181] operators of commercial websites and online services directed to or 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.

Telemarketing and Consumer Fraud and Abuse Prevention Act:[182] This Act requires the FTC to enact 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.

Do-Not Call Registry Act:[183] This Act 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:[184] This Act establishes requirements for those who send unsolicited commercial email, 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.

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

---

[180] 15 U.S.C. §§ 6501-6506; see http://www.ftc.gov/privacy/coppafaqs.shtm.

[181] Codified at 16 C.F.R. Part 312.

[182] 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.

[183] The Do-Not Call Registry Act of 2003 (15 U.S.C. § 6151; originally codified at 15 U.S.C. § 6101 note): http://www.gpo.gov/fdsys/pkg/USCODE-2010-title15/pdf/USCODE-2010-title15-chap87A-sec6151.pdf

[184] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) (15 U.S.C §§ 7701-7713): http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

Health Insurance Portability and Accountability Act (HIPPA):[185] HIPAA provides federal protections for personal health information held by "covered entities," which 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 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:[186] Under this Rule, 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:[187] 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.

Americans with Disabilities Act (ADA):[188] 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

---

[185] HIPAA and its implementing regulations issued by the U.S. Department of Health and Human Services (the "Privacy Rule" and the "Security Rule"). 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.

[186] Health Information Breach Notification Rule (Health and Human Services) 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.

[187] Health Breach Notification Rule (Federal Trade Commission), 16 CFR Part 318, available at http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule.

[188] Pub. L. 101-336, as amended. Titles I and V of the ADA are online at http://www.eeoc.gov/laws/statutes/ada.cfm.

confidential medical record.[189] The EEOC issues additional guidance on employment-related inquiries.[190]

Genetic Information Nondiscrimination Act (GINA):[191] 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 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.[192]

Title X of the Public Health Service Act, Confidentiality of Title X Service Information:[193] 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:[194] 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.

---

[189] 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).

[190] 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.

[191] 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

[192] 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

[193] 42 C.F.R. § 59.11, available at http://law.justia.com/cfr/title42/42-1.0.1.4.41.1.19.11.html.

[194] 42 CFR Part 2 and 42 USC § 290-dd-2, available at http://www.samhsa.gov/legislate/Sept01/01907_42cfr_part2.htm.

Medicaid Privacy Requirements:[195] 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):[196] The FDCA provides that 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 the subject will be maintained and that notes the possibility that the Food and Drug Administration may inspect the records.

Controlled Substances Act (CSA)**:**[197] The 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):[198] 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

---

[195] 42 CFR §§ 431.300-307 and 42 USC 1396a(a)(7), available at https://www.emedny.org/epaces/MedConfidentialityReg.aspx#Question_1.

[196] 21 CFR Part 50 available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=50.

[197] 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.

[198] 45 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.

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.[199]

Statutory Authority for Certificates of Confidentiality:[200] 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.

Patient Safety Act:[201] This 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:[202] 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)

---

[199] http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html.

[200] 42 U.S.C. 241(d), available at http://www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000241----000-.html.

[201] Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act); 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).

[202] 12 CFR Part 717, available at http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr717_06.html.

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:[203] 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:[204] 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:[205] 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 protect the confidentiality of customers' personal information, and limits the power of such entities to use or disclose that information.[206] 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.[207] The Act also prohibits unauthorized interception and publication of communications made by wire or radio.

Telephone Consumer Protection Act (TCPA),[208] as amended by the Junk Fax Prevention Act,[209] and the Controlling the Assault of Non-Solicited Pornography and Marketing:[210] 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

---

[203] 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.

[204] 42 U.S.C. § 242m(d) available at http://www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000242---m000-.html.

[205] 47 U.S.C. § 151 et seq., available at http://transition.fcc.gov/telecom.html.

[206] 47 U.S.C. §§ 222, 338(i), 551.

[207] *See* 47 C.F.R. § 64.1601(b).

[208] Codified as 47 U.S.C. § 227.

[209] *Id.*

[210] 15 U.S.C. 7701, et seq., Public Law No. 108-187.

unwanted commercial email messages to wireless devices without prior permission. The FCC jointly enforces these statutory provisions with the FTC.[211]

Drivers Privacy Protection Act of 1994 (DPPA):[212] 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).[213] The 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.

Family Educational and Privacy Rights Act (FERPA).[214] 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):[215] 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

---

[211] 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.

[212] 18 U.S.C. § 2721 et seq.

[213] 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).

[214] 20 U.S.C. § 1232g.

[215] 20 U.S.C. § 1232h; 34 CFR part 98.

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):[216] 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.[217] 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.[218]

STATE LEGISLATION: 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.[219] In general, the fifty states have a variety of privacy /data protection laws dealing with: patient access to their medical records; restrictions on disclosure of identifiable medical records; rules relating to confidentiality-privilege of records documenting communications between patients and health care professionals including mental health professionals; and condition-specific laws which target certain medical conditions. 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.[220]

---

[216] 18 U.S.C. § 2710.

[217] "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").

[218] White Paper, at pp. 35-39.

[219] 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. A sampling of representative state laws: Minnesota statutes on internet privacy §§ 325M.01 to .09: http://www.revisor.leg.state.mn.us/stats/325M; Nevada statute on privacy requirements for internet service providers § 205.498, available at: http://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec498; California requirements on disclosures for third party sharing §§ 1798.83 to .84: available at http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84; California's Online Privacy Protection Act §§ 22575-22578, available at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579; Utah requirements on disclosures for third party sharing §§ 13-37-101, -102, -201, -202, -203; available at: http://le.utah.gov/~code/TITLE13/13_37.htm; Delaware requirements for employer notice of email/Internet monitoring § 19-7-705, available at: http://delcode.delaware.gov/title19/c007/sc01/index.shtml#705; Connecticut requirements for employer notice of electronic monitoring § 31-48d, available at: http://www.cga.ct.gov/2011/pub/chap557.htm#Sec31-48d.htm; Connecticut privacy policy requirement § 42-471, available at: http://www.cga.ct.gov/2011/pub/chap743dd.htm#Sec42-471.htm; Nebraska requirement related to statements in privacy policies § 87-302(14), available at: http://uniweb.legislature.ne.gov/laws/statutes.php?statute=87-302; Pennsylvania requirement related to statements in privacy policies 18 Pa. C.S.A. § 4107(a)(10), available at: http://government.westlaw.com/linkedslice/default.asp?SP=pac-1000.

[220] Available at http://hpi.georgetown.edu/privacy/publications.html.

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.[221]

iii. Habeas Data:

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.[222]

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, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[223]

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.[224]

iv. Self Regulation:

In the United States, the FTC has generally 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."

---

[221] White Paper, at pp. 37-38.
[222] 15 U.S.C. § 1681g, available at http://www.ftc.gov/os/statutes/031224fcra.pdf. and *See, e.g.,* section 609 of FCRA (Disclosures to Consumers).
[223] FRCP Rule 26 Duty to Disclose, available at http://www.law.cornell.edu/rules/frcp/rule_26.
[224] See state-level overview at http://sunshinereview.org/index.php/State_sunshine_laws.

Industry initiatives include examples such as the Codes of Conduct for the Mobile Marketing Association[225] and the Interactive Advertising Bureau.[226] 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.[227] Key stakeholders have also come together 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[228/] 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

---

[225] See http://mmaglobal.com/policies/code-of-conduct.
[226] See http://www.iab.net/public_policy/codeofconduct.
[227] 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.
[228] Documents online at http://export.gov/safeharbor/.

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.

The Obama Administration White Paper has also 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).

B. Enforcement

i. Enforcement and Recourse:

Legislation on privacy/data protection at the federal and state level provides specific rights of action, procedures and remedies as follows:

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.[229] The FCRA also provides for criminal sanctions for obtaining consumer report information under false pre-tenses.[230] The Act is

[229] 15 U.S.C. §§ 1681n, 1681o
[230] 15 U.S.C. § 1681q

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.[231]

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.[232]

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.

Telemarketing Act:[233] The FTC also enforces the Telemarketing Act, under which it promulgated and enforces the Telemarketing Sales Rule ("TSR"),[234] 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.[235] 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.[236]

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.[237]

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.

---

[231] 15 U.S.C. § 1681s(a)
[232] 15 U.S.C. § 6805
[233] 15 U.S.C. §§ 6101-6108
[234] 16 C.F.R. Part 310
[235] 15 U.S.C. §§ 53(b), 57b, 6102(c), and 6105(b)
[236] See FCC website at http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email
[237] *See* 47 C.F.R. § 64.3100.

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: 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.[238]

Communications Act: Under the Communications Act, a person whose privacy rights were violated by a telecommunications carrier may file a complaint with the FCC,[239] or seek damages in federal court,[240] but may not pursue both remedies.[241] 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.[242] 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.[243] 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.[244]

Any person who willfully and knowingly violates the prohibition in the Communications Act,[245] intercepts and publishes communications made by wire or radio is subject to possible fines or imprisonment.[246] Any person who willfully and knowingly violates a regulation made pursuant to the Communications Act may be fined.[247] 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.[248]

---

[238] Section 12117 (ADA section 107).
[239] 47 U.S.C. § 208
[240] 47 U.S.C. §§ 206
[241] 47 U.S.C. § 207
[242] 47 U.S.C. § 205
[243] 47 U.S.C. §§ 338(i)(7), 551(f)
[244] 47 U.S.C. § 227
[245] 47 U.S.C. § 501
[246] 47 U.S.C. § 605(e)
[247] 47 U.S.C. § 502
[248] 47 U.S.C. § 503

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.[249] The Electronic Communications Privacy Act imposes civil liability. Courts may award damages, attorneys' fees and costs.

Family Educational Rights and Privacy Act (FERPA).[250] FERPA is administered by the Family Policy Compliance Office (FPCO) in the U.S. Department of Education,[251] which 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.[252] 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.[253] 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.

Protection of Pupil Rights Amendment:[254] The PPRA is also administered by the Family Policy Compliance Office (FPCO) in the Department of Education. PPRA does not provide for a private 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. Neither FERPA nor the PPRA provide for a private right of action.[255]

Telephone Consumer Protection Act: Under the 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.[256]

Drivers Privacy Protection Act: The DPPA provides for criminal fines and civil penalties. It is enforced by federal authorities as well as private litigants.[257]

---

[249] 47 U.S.C. § 503

[250] Section 444 of the General Education Provisions Act (GEPA), commonly referred to as the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR part 99.

[251] *See* U.S. Department of Education website at http://www2.ed.gov/policy/gen/guid/fpco/index.html.

[252] 20 U.S.C. § 1234c(a).

[253] 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).

[254] General Education Provisions Act (GEPA), section 445, commonly referred to as the Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h; 34 CFR part 98.

[255] 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.

[256] *See* 47 U.S.C. §§ 227(b)(3), (c)(5).

[257] 18 U.S.C. §§ 2723, 2724.

Judicial remedies for state-level causes of action for privacy torts are generally available but can vary between states. [258] In addition, the fifty states have a variety of privacy /data protection laws dealing with the following issues, which also provide specific remedies and causes of action : 1) patient access to their medical records;[259] 2) restrictions on disclosure of identifiable medical records;[260] 3) rules relating to confidentiality-privilege of records documenting communications between patients and health care professionals including mental health professionals;[261] and 4) condition-specific laws which target certain medical conditions. Each category of law has its state specific remedies, penalties, and fines.[262]

Data is not readily available on all of the other federal and state statutes containing privacy/data protection or which may contain provisions for judicial redress.

---

[258] 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.

[259] 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.

[260] 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 § 9-340C(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.

[261] 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)].

[262] 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].

ii. Data Protection/Enforcement Authorities:

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.

FTC 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.

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.

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. The Office for Human Research Protections (OHRP) also 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.

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

iii. Investigatory Capabilities/Criminal Prosecution:

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. The FTC does not address each individual complaint. Instead, the FTC exercises its prosecutorial discretion in selecting enforcement matters.

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.

Department of Health and Human Services: 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.

Office for Human Research Protections: 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;[263] (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).

With regard to complaints subject to potential criminal prosecution: the FCRA provides for criminal sanctions for obtaining consumer report information under false pre-tenses;[264] the ECPA establishes that certain violations may carry criminal liability;[265] the Communications Act

[263] 45 CFR 46.103(b)(5)
[264] 15 U.S.C. § 1681q.

[265] 18 U.S.C. § 2511(4). *See also* 18 U.S.C. § 3121(d) (criminal penalties for Pen/Trap statute violations).

provides that any person who willfully and knowingly violates a provision of the Communications Act may be both fined and sentenced to imprisonment;[266] and HIPAA authorizes the U.S. Department of Justice (DOJ) to enforce criminal violations of that act. In this latter case, 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.

Data is not readily available for state enforcement authorities.

C. Cross-Border Cooperation

i. Data Transfer:

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

ii. International Instruments/Arrangements:

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.

The United States has also 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.

ii. Cross-Border investigatory and enforcement cooperation:

Information Sharing: 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.

[266] 47 U.S.C. § 501.

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; 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.

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.

Enforcement Cooperation: Under the U.S. SAFE WEB Act, the FTC may also 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.

D. Case Law and Special Challenges

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.[267] Courts have also recognized that individuals have substantive privacy interests against private parties.[268]

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.[269] 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.[270]

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 multi-stakeholder 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

---

[267] *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.").

[268] *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).

[269] *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.

[270] 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).

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.

11. URUGUAY: