Asia-Pacific
Economic Cooperation

APEC Cross-Border Privacy Rules System Implementation: Peru

Electronic Commerce Steering Group
APEC Committee on Trade and Investment

February 2013

APEC Project CTI 01/2011T

Produced by
Lucy L. Thomson, Esq., Washington D.C. as part of the APEC Cross-Border Privacy Rules System Implementation and Administration Assistance project.

For
Asia Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#213-CT-01.2

Table of Contents

This Report was prepared for the APEC Secretariat by Lucy L. Thomson, Esq., Washington D.C. as part of the APEC Cross-Border Privacy Rules System Implementation and Administration Assistance project. She would like to acknowledge the substantial contributions of Professor William J. Luddy, Jr.

INTRODUCTION

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework is a set of nine principles[1] to assist APEC economies in developing privacy approaches that maximize privacy protection and the continuity of cross-border information flows. The APEC Privacy Framework states that international implementation of these principles may be achieved through the Cross-Border Privacy Rules (CBPR), a set of voluntary rules based upon the APEC privacy principles. The organization may then commit to applying these rules to its activities involving transfers of personal information across borders.

At the outset, we acknowledge the important commitment Peru has demonstrated to the APEC Data Privacy Pathfinder. Peru became a member of APEC in 1998 and hosted the 2008 APEC meetings. The Peruvian Congress enacted Law 29733 Protection of Personal Data (*Ley de Protección de Datos Personales*) in 2011 to strengthen existing data protections. A proposed implementing regulation for the data protection law was published for public comment in September 2012. In 2006 Peru published an Information Privacy Individual Action Plan that described how it was advancing each of the principles of the APEC Privacy Framework through its Constitution, laws, and regulations.[2]

Peru officials have indicated their interest in participating in the APEC CBPR System, given the broad privacy protections in the Peru data protection law and the proposed implementing regulation. They requested assistance from the APEC Secretariat to move towards completion of the required steps in the CBPR process.[3] Consultations were held on August 13-14, 2012 in Lima, Peru with attorneys and other officials of the Peru Ministry of Justice and the Ministry o Foreign Trade and Tourism (MINCETUR). This group included members of Peru's delegation to the APEC Electronic Commerce Steering Group (ECSG) and its Data Privacy Subgroup (DPS). These consultations were very useful in developing an understanding of Peru's approach to data privacy and the steps it has already taken to become compliant with the APEC Data Privacy Framework and to participate in the APEC Pathfinder program.

Following an ambitious two-day agenda,[4] the participants were able to accomplish the goals of developing a thorough understanding of the APEC CBPR System requirements, analyzing the sufficiency of existing Peru privacy laws, regulations and directives, and completing an initial draft of the CBPR enforcement map.

---

[1] These principles are: Preventing Harm, Notice, Collection Limitation, Use of Personal Information, Choice, Integrity, Security Safeguards, Access and Correction, Accountability.

[2] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx

[3] The United States' participation in the CBPR System provides an instructive example of the documentation required to be submitted. *See* http://web.ita.doc.gov/ITI/itiHome.nsf/5713559d82a954b085256cc40075a766/b256a0f35cf9ecc885257a480043d1eb/$FILE/United%20States%20CBPR%20Findings%20Report.pdf

[4] *See*, Appendix A attached to this Report.

This Report reviews the data privacy framework in Peru and considers an approach for an Accountability Agent and the Enforcement Authority that would be consistent with Peru's domestic legal regime and its historic approach to regulation. Implementation of the APEC Data Privacy Framework should strengthen electronic commerce activities in Peru by enhancing 'trust' among consumers and businesses for conducting business online. It will also help to increase growth and development of Peruvian businesses that wish to market their products and services across borders.

PERU PROFILE

Peru is the third-largest economy in South America. Located on the Pacific Ocean, it stretches more than 2,875 kilometres from Ecuador on the north to Chile to the south. Its eastern border is shared with Colombia, Brazil, and Bolivia. Peru's terrain is extraordinarily diverse, consisting of western and coastal plains, central rugged Andean mountains, and eastern lowlands with tropical forests that are part of the Amazon basin.

The fifth-most populous economy in Latin America, Peru's population was estimated to be 30.0 million in 2011, with 75 percent of the Peruvian people living in urban areas. Thirty percent (30) of the population lives in the metropolitan area of Lima, the capital of Peru.[5]

Peru has abundant natural resources, including minerals (silver, copper, zinc, tin, lead, gold, and iron ore), fish, petroleum, natural gas, and forestry products. Its economy consists of manufacturing (15 %), agriculture (7.5 %), services (55.6 %), mining (6.2 %), construction (6.7 %), and fisheries (0.3 %). About 17.5% of Peru's total revenues come from commodities. It exports approximately $35 billion in gold, copper, fishmeal, zinc, textiles, apparel, asparagus, coffee and other products to its major markets—the United States (16.3 %), China (15.5 %), Switzerland (11.0 %), Canada (9.5 %), Japan (5.1 %, Germany (4.3 %), Chile (3.9 %), and Spain (3.3 %). Its imports of $27.91 billion come primarily from the United States, China, Brazil, Ecuador, Japan, Columbia, and Mexico.

One of the best-performing economies in Latin America, Peru has achieved remarkable economic growth over the past decade.[6] Peru's GDP growth has averaged 6.3 percent between 2002 and 2012. Peru's per capita income increased by more than 50 percent during the decade.[7] "Stimulated by a favourable external environment and the government's commitment to political

---

[5] U.S. Department of State, Fact Sheet-Peru, August 28, 2012, *available at* http://www.state.gov/r/pa/ei/bgn/35762.htm.

[6] The World Bank, Peru Overview, *available at* http://www.worldbank.org/en/country/peru/overview.

[7] *Id*., The World Bank, Country Partnership Strategy FY12-FY16, "Peru is one of the best performing economies in Latin America and the new Country Partnership Strategy between Peru and the World Bank focuses on supporting national priorities and improving equity through social services, infrastructure and competitiveness."

and economic stability, Peru's economy has recorded since 2002 the fastest growth in South America." [8]

Currently the Government is committed to addressing the challenge of achieving more inclusive economic growth. It has been pursuing an economic agenda focused on six key areas: (i) maintaining macroeconomic stability and reducing vulnerabilities (Peru is prone to frequent natural disasters); (ii) accelerating growth and widening its base; (iii) making growth more economically sustainable (with particular focus on fisheries and mining); (iv) meeting basic needs (expansion of electricity, water and sanitation); (v) promoting and developing a new social contract in education, health, and nutrition; and (vi) modernizing state institutions (reforming the justice system to ensure independence, transparency and integrity, and enhancing access to justice services).[9]

Peru is strongly committed to free trade and has welcomed large amounts of foreign investment.[10] It has signed bilateral investment treaties with most of its North and South American neighbors and a number of European and Asian economies. It has signed free trade agreements (FTA) with economies that include the United States in 2006 and Chile, Mexico, Canada, Singapore, China, the European Union (EU), Korea, Japan and the European Free Trade Association (EFTA),and it is currently negotiating the Transpacific Partnership Agreement (TPP) .[11]

ELECTRONIC COMMERCE DEVELOPMENTS

The development of electronic commerce in Latin America has exceeded expectations, reaching $43 billion in 2011, compared with $22 billion in 2009, representing a growth rate of 98%. This is the result of innovative ideas and the use of new tools – the online channel, new players (coupon firms), and new business models.[12] One third of Peru's population is active on the Internet connecting via social networks.

Peru has experienced a 1.4% growth in the volume of e-commerce transactions.[13] Internet users in Peru totaled nearly 10 million in 2010, up from 8.7 million in 2008. Broadband Internet

---

[8] OECD Investment Policy Reviews: Peru (OECD 2008), *available at* http://www.oecd.org/daf/internationalinvestment/investmentpolicy/41715631.pdf.

[9] *Supra* n. 6, The World Bank, Peru Overview.

[10] Id.

[11] Id.

[12] Latin America's Bouyant e-Commerce Sector Prepares to Go Mobile, Knowledge@Australian School of Business (August 12, 2012), *available at* http://knowledge.asb.unsw.edu.au/

[13] Id.

subscribers jumped from half to three quarters of a million subscribers in 2011.[14] Information and communication technology (ICT) expenditures increased per capita to $153.6 from $119. With a 35% e-commerce growth rate in the Latin American region, there is great potential for Peru to take advantage of and participate in this strong growth.

In addition, Peru has enacted laws that will support expansion of its digital economy, including a law that authorizes the use of digital certificates and signatures for electronic contracts,[15] a computer crime law that prohibits the unlawful access, use, interference, or damage to a system, database, or network of computers,[16] and a law that regulates the use of unsolicited commercial e-mails (spam).[17]

ACCOUNTABILITY AGENT AND ENFORCEMENT AUTHORITY PRINCIPLES

The APEC Ministers have endorsed the APEC Privacy Framework (2004) as well as the APEC Data Privacy Pathfinder (2006). A key issue for APEC member economies is how each will enforce the framework. This is, of course, a matter for domestic law and regulation. The legal framework must also take into account the important cross-border aspects of the APEC Data Privacy Pathfinder

In establishing an Accountability Agent, the Government must identify existing law or establish new laws and/or regulations that provide the legal basis for the particular Accountability Agent model to be implemented. Generally, there are three models. First is the "public sector" model under which a government agency or regulator is the Accountability Agent.[18] Another is the "private sector" model under which a private sector organization or organizations undertakes the responsibilities of the Accountability Agent. Under the third model—perhaps a subset of the second—a professional firm, such as an auditing firm, law firm, etc., can be accredited as an Accountability Agent.

The Accountability Agent, whether public or private, is responsible for assessing and evaluating private sector organizations that voluntarily seek approval to use the APEC privacy seal or

---

[14] The World Bank, Data, *available at* http://data.worldbank.org/country/peru.

[15] Laws 27269 and 27291–Electronic Contracts–authorize the use of digital certificates and signatures for electronic contracts, and set conditions for rescission of the contracts. Law 27291 was modified in 2000 to recognize the legal value of electronic contracts and electronically authorized transactions such as those conducted through branchless banking channels..

[16] *Supra* n. 6, The World Bank, Country Partnership Strategy.

[17] Law No. 28493 regulates the use of unsolicited commercial e-mails (spam). Spam that originates in Peru must contain certain information in the subject of the e-mail, identification of the natural or legal person who send the spam, and a valid e-mail address that can be used to opt-out. If the spam does not comply with these requirements, contains false or misleading information, or if the sender does not comply with opt-out requests, individuals may seek damages for the violations.

[18] *See, e.g.,* Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) that adopted fair information principles and established a Privacy Commissioner, *available at* http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

trustmark. It verifies that the privacy policies and practices of companies seeking CBPR certification meet the baseline requirements of the system. The assessment entails a careful review[19] of responses to the Pathfinder Intake Questionnaire submitted to the Accountability Agent. The questionnaire consists of 50 questions that reflect each of the principles in the APEC Data Privacy Framework. Once an entity has been approved to use the APEC data privacy trustmark, it will undergo periodic audits by the Accountability Agent to ensure that it continues to comply with the Pathfinder. If an entity is found not to be in compliance, whether through a periodic review or as a result of the Accountability Agent's investigation of a complaint, the Agent may revoke the authority to use the trustmark.

In addition, a member economy must establish the Enforcement Authority in order to participate in the APEC Data Privacy Pathfinder. The member economy must identify the appropriate regulator (or ministry) that will sign the APEC Enforcement Cooperation Arrangement that was endorsed by the Electronic Commerce Steering Group (ECSG).[20] The Enforcement Cooperation Arrangement specifies that the signatory is the public entity with the legal authority and responsibility for enforcing an APEC member economy's privacy laws. It describes privacy laws as "those laws, *the enforcement of which* would have the effect of protecting personal information consistent with the APEC Privacy Framework." [*Emphasis added*.] It should be noted that the Privacy Enforcement Authority is an essential part of any data privacy protection regime, not just the APEC CBPR System. Establishing the legal framework for the Enforcement Authority is a critical step in implementing the APEC Data Privacy Pathfinder.

Finally, when developing the legal framework for an Accountability Agent and the Enforcement Authority, it is very useful to designate one government authority to lead the process for modifying existing law. This agency or other entity would be responsible for a number of functions. For example, it would draft legislation and prepare appropriate regulations. It would collaborate with other government ministries and agencies involved in implementing the APEC Data Privacy Pathfinder. Most important, it would be responsible for moving forward the process of implementing the Data Privacy Pathfinder in the member economy.

IMPLEMENTING THE CBPR SYSTEM IN PERU

Legal Framework–Current Data Privacy Environment

This section of the Report focuses on Peru's legal and regulatory framework. The consultations with Peruvian officials provided an opportunity to assess whether their laws are sufficiently broad to form the underlying legal basis for a comprehensive data privacy regime and how they may be used to enforce the APEC Privacy Framework and support the establishment of an Accountability Agent and the Enforcement Authority.

---

[19] An assessment methodology that is consistent across all economies participating in the APEC Data Privacy Pathfinder is used.

[20] *See* http://www.apec.org/apec/news___media/fact_sheets/201006cpea.html.

Peru Law 29733–Protection of Personal Data (*Ley de Protección de Datos Personales*) was enacted in 2011 to strengthen existing data protection policies.[21] This overarching privacy law provides broad privacy protections and creates a National Authority for Protection of Personal Data with responsibility for private sector data privacy protection. A proposed regulation to implement the data protection law was published for public comment in September 2012. Thus, the data protection law explicitly establishes the Enforcement Authority. Peruvian officials will need to determine what Accountability Agent model they will adopt, and draft the regulation or policy necessary to establish it.

The major laws[22] relevant to data privacy in Peru are described briefly below. In addition to laws that specifically address privacy, Peru has enacted consumer protection laws that cover broad industry sectors. The enforcement mechanisms in these laws may provide models that also could be applied to the Accountability Agent and Enforcement Authority functions.

Political Constitution of Peru–Article 2

Peru's Constitution enunciates the fundamental right to protection of personal data (paragraph 6):

> "Every person has the right:
>
> "To be assured that information services, whether or not they are computerized, public or private, will not release information affecting one's personal and family intimacy.
>
> "To his honor and good reputation, personal and family intimacy, and his own voice and image. Every person affected by inaccurate or injurious statements contained in any medium of social communication has the right to free, immediate and proportional rectification, notwithstanding other legal responsibilities.
>
> "To freedom of information, opinion, expression, and the dissemination of thoughts through the spoken or written word or in images, by any means of social communication, and without previous authorization."

Law No. 29733–Law on Protection of Personal Data

The Law on Protection of Personal Data (*Ley de Protección de Datos Personales*) provides a broad range of privacy rights in Peru, including rights that are consistent with the APEC Data Privacy Framework.[23] This law is intended to guarantee the fundamental right to protection of personal data (Constitution Article 2.6) through its proper treatment within a framework of respect for other fundamental rights that the law recognizes. The law provides privacy rights to

---

[21] *See, generally* https://www.privacyinternational.org/reports/peru. The Information Privacy Individual Action Plan (2006) identified Peru laws in effect at the time that were relevant to each of the APEC Privacy Principles.

[22] It should be noted that not all official versions of the laws and regulations discussed were available in English.

[23] Unofficial English translation *available at* http://web.ita.doc.gov/ITI/itiHome.nsf/9b2cb14bda00318585256cc40068ca69/112a1a2f4d01989c85257a78004dd2ec?OpenDocument.

individuals through eight "guiding principles" that include Legality, Consent, Finality, Proportionality, Quality, Security, Enforcement, and Restriction on Cross-Border Transfers. The law follows the approach of the European Union Data Protection Directive and the Spanish Data Protection Acts of 1992 and 1999. It was enacted in June 2011 and became effective in April 2012.

For example, Title I of the law provides that personal data may only be processed with the prior, informed, explicit and unambiguous consent of the data owner. In the case of sensitive data, consent must be in writing. Further, personal data may only be used for the purposes for which it was collected. Data owners also have rights to have the data corrected, eliminated, or blocked in the event that it is incorrect or in error. Article 15 addresses transborder flows of personal data, and requires that recipient economies maintain adequate levels of protection of personal data under the data protection law.

Other sections of the law provide obligations for holders of private data, such as banks and other financial institutions, in commercial transactions; the processing of personal data by public bodies; and penalties for violation of the law. With respect to enforcement and sanctions, the law provides data subjects the "right to protection" through an action in habeas data.[24]

National Authority for Protection of Personal Data

Article 32 of the data protection law created the National Authority for Protection of Personal Data ("National Authority") with responsibility to implement and enforce the law, including monitoring compliance with the requirements related to the trans-border flow of personal data. It is located in the National Directorate of Justice of The Ministry of Justice.

The National Authority has been given broad responsibility and power to carry out the following administrative, guiding, regulatory, decision-making, supervisory and sanctioning functions:[25]

1) Represent the economy to the international instances in matters of personal data protection.
2) Cooperate with foreign authorities for personal data protection in order to carry out their tasks and generate bilateral and multilateral cooperation mechanisms for mutual assistance and due mutual help when required.
3) Administer and keep updated the National Register of Personal Data Protection.
4) Publicize through the Institutional Portal the updated list of publicly and privately-

---

[24] CONST. Peru, article 200, subsection 3. Habeas data is a constitutional guarantee that protects against any act or omission by whatever authority, whether a state employee or a private person, that would reduce or jeopardize the rights of the individual as contained in Article 2, Subsections 5-6 of the Peruvian Constitution. The constitutional procedure of habeas data protects not only the right of a person to access information about himself (right to informational self-determination) (Constitution, Article 2.6), but also the right to access whatever information an individual may require from any public body (freedom of information and access to government records) (Constitution, Article 2.5). The Code of Constitutional Procedures provides the procedures for habeas data (2004).

[25] Supra, n. 23, Article 33.1–33.20.

administered personal data databases.

5) Promote campaigns of spreading and promotion concerning personal data protection.
6) Promote and reinforce a culture of protection of the personal data of children and adolescents.
7) Coordinate the inclusion of information about the importance of private life and personal data protection in the curricula of the schools at all levels and also support the training of teachers on these topics.
8) Issue authorizations, when applicable, pursuant to the regulation of this Law.
9) Answer questions about personal data protection and the meaning of the current rules in the matter, especially those issued by it.
10) Issue a technical opinion concerning the bills referring in full or in part to personal data, which will be binding.
11) Issue the corresponding guidelines for the better application of the provisions of this Law and its regulation, especially in matters of security of personal data databases and supervise compliance therewith, in coordination with the sectors involved.
12) Promote the use of self regulation mechanisms as an additional instrument for personal data protection.
13) Execute inter-institutional and/or international cooperation agreements in order to assure the rights of the persons in matters of personal data protection processed in and out of the national territory.
14) Process requests for the private interest of the citizen or the general interest of the community, as well as requests for information.
15) Hear, investigate and resolve the complaints lodged by the data subjects for the violation of the rights granted to them and issue provisional and/or corrective measures, as established in the regulation.
16) Assure compliance with the laws related to personal data protection under respect of their guiding principles.
17) Obtain from the controllers of personal data databases the information it deems necessary for compliance with the rules on personal data protection and the performance of its functions.
18) Supervise the personal data processing carried out by the controller and processor of the personal data databases and, in case of illegality, order the appropriate actions, pursuant to the Law.
19) Start investigations, ex officio or by complaint of a party, for presumed acts contrary to the provisions of this Law and its regulation and apply the corresponding administrative sanctions, without prejudice to the provisional and/or corrective measures established by the regulation.
20) The other functions assigned to it by this Law and its regulation.

As a public body in Peru that is responsible for enforcing the privacy laws and regulations of an APEC economy consistent with the APEC Data Privacy Framework, the National Authority would fulfill the functions of the APEC Privacy Enforcement Authority.

Proposed Regulation for the Law on Protection of Personal Data

The Ministry of Justice published a proposed regulation to implement the data protection law. Title II of the regulation sets forth four "guiding principles" of personal data protection to which the holder of databases and/or the data controller must comply: Consent, Purpose, Quality and Security. Other topics in the regulation include personal data processing (Title III), rights of the personal data holder (Title IV), National Register of Personal Data Protection (Title V), and violations and sanctions (Title VI).

The regulation names the General Department of Personal Data Protection as the new office in charge of implementing the data protection law. However, the regulation does not explicitly create an Accountability Agent system under the regulatory powers provided to the National Authority. It will be important for Peruvian officials to determine whether an explicit authorization is required.

The data protection law and regulation would strengthen the substantive protections for individuals (and legal entities) in the privacy arena. They emphasize the right of citizens to control their own personal information. In this regard, the drafters of the legislation appear to have been influenced by the APEC Privacy Framework,[26] as well as the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[27] which is the basis for the APEC Data Privacy Framework. Depending on the final version of this proposed regulation, it is likely that it will provide much of the legal infrastructure needed for Peru's participation in the APEC Pathfinder program.

Title IV of the regulation (Chapter III) creates a protection procedure with the General Department of Personal Data Protection for data subjects to pursue complaints against the holder of a database or data controller for alleged violations of privacy rights. Title VI specifies the violations that may be investigated and sanctions imposed by the Department of Supervision and Control or the General Director of Personal Data Protection. The Director of Sanctions and the General Director of Personal Data Protection may pursue the application of sanctions under procedures in Title VI Chapter II and the sanctions specified in Chapter III. In addition, the regulation provides requirements for security and access control, and the authority to levy fines on both public and private organizations that do not provide appropriate levels of security for personal data that may be collected and/or stored in databases.

Law No. 27806 modified by Law No. 27927–The Law of Transparency and Access to the Public Information

This law governs the rights of citizens to access public information and information controlled by juridical persons. It incorporates the principle of publicity, which provides that all activities and provisions of "public" administration, as well as all government information, are presumed to have free access.

---

[26] http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

[27] *Supra*, n. 8.

Law Nos. 25868/92 and Law Decree 691–Consumer Protection

The Consumer Protection Law establishes the basic legal framework and standards for marketing to consumers. Enforcement responsibilities are divided between the Peru Superintendent of Banks, Insurance, and AFPs (SBS), which concentrates its efforts on preventative measures, primarily transparency (disclosure of clear, explicit, comprehensible, visible, and precise pricing information to clients and the public for the most commonly used financial services), and the National Institute of Defense of the Competition and Protection of Intellectual Property (INDECOPI), which focuses its attention on corrective actions, solving problems and disputes between consumers and financial service providers.

SBS does not solve individual disputes between consumers and providers (except in the private pension system), but it has a mechanism to receive consumer complaints on the transparency resolution. However, SBS regulates and supervises the policies and procedures set by financial institutions to receive, manage, and properly resolve complaints. It has the legal authority to actively identify and curb/prohibit predatory or abusive practices and to impose sanctions on financial institutions.

INDECOPI, through its Tribunal for the Defense of Competition and Intellectual Property, has enforcement authority over rules pertaining to competition, consumer protection, and intellectual property rights in all sectors and industries, including financial services. Its enforcement powers include the authority to conduct investigations, impose corrective measures, and levy sanctions. INDECOPI works to resolve disputes between consumers and providers. This dispute resolution process is a required step before a consumer may seek judicial review.

Both SBS and INDECOPI have supervisory and sanctioning powers under the financial transparency regulation and the consumer protection law, respectively.

While these entities are not focused specifically on data protection issues, it is possible that complaints that are made to these organizations may have data privacy issues, including cross-border data privacy issues, associated with them. The collaboration between these entities and the Privacy Enforcement Authority (within the Justice Ministry) will need to be addressed going forward.

Mechanisms for Grievance Resolution–Ombudsman

The financial sector in Peru has a process for grievance redress, including an Ombudsman–the Financial Client Defender–set up by the bank association, which offers free arbitration or mediation between clients and financial institutions.[28] SBS created a complaint filing mechanism for financial users to receive complaints and screen and forward them to INDECOPI when appropriate. SBS may initiate inspections and impose sanctions on financial institutions for lack

[28] *Financial Inclusion and Consumer Protection in Peru*, Joint assessment report, Superintendent of Banks, Insurance and AFPs (February 2010) *available at* http://www.cgap.org.sites/default/files/CGAP-Financial-Inclusion-and-Consumer-Protection-in-Peru-Feb-2010.pdf.

of compliance with applicable rules. In addition, consumers may file complaints directly with INDECOPI. Consumers may appeal a decision by INDECOPI to the Tribunal for the Defense of Competition and Intellectual Property, an independent body within INDECOPI. The office also responds to consumer questions and publicizes its decisions on its website. An institution found to have committed a violation is subject to a fine of up to 10 percent of its sales or revenues of the previous tax year.

As in the case of Peru's Consumer Protection law, there may be instances where complaints brought to the Ombudsman may need to be coordinated with the Privacy Enforcement Authority.

Protection of Data in Credit Reports

A Peru law regulates private credit reporting agencies that collect and process the credit risk information of individuals and companies whose information is recorded in databases.[29] The law requires that information must be provided to the data subject when the data has not been obtained from him or her. It prohibits credit bureaus from collecting sensitive information, data violating the confidentiality of bank or tax records, inaccurate or outdated information, bankruptcy records older than five years, and certain records after a debt has been paid. The Agency for Consumer Protection in INDECOPI has the authority to impose fines for violations of the law, and can issue injunctions to correct errors. Thus, coordination with the Privacy Enforcement Authority may need to be developed in this area.

Privacy of Telecommunications

The Law of Telecommunications states that all persons have the right to the inviolability and secrecy of their telecommunications. The Ministry of Transports, Communications, Housing and Construction is responsible for protecting this right.[30]

COMMENTARY

The importance of cross-border data privacy protection in international trade development has increased significantly over the past decade. The APEC Data Privacy Pathfinder provides to Peru and other APEC member economies the opportunity to participate in an *enabling* data privacy approach that seeks to protect privacy rights while facilitating cross-border data flows that are important to the efficient functioning of global supply chains and business development.

A successful data privacy regime will provide competitive advantages to Peru's trade development efforts and to Peruvian businesses seeking to enhance and increase their international business activities. Developing a privacy infrastructure through participation in the

---

[29] Centrales Privadas de Informacion de Riesgos (CEPIRS). http://www.leyes.congreso.gob.pe/CodigoP.htm. Law No. 26702-General Financial System and the Insurance System and the Organic Law of the Banking and Insurance Superintendent's Office (6/12/96, modified 5/6/99 Arts. 140-143). *See* http://www1.worldbank.org/finance/assets/images/Regulation_of_Personal_Data_Protection.pdf.

[30] *See* http://www.tc.gob.pe/

APEC Data Privacy Pathfinder and continuing to move forward with participation in the CBPR System should enable Peru and Peruvian businesses to compete even more successfully for the new trade and business development they are pursuing.

Some of the considerations Peruvian policy-makers may wish to take into account in moving forward with the APEC Data Privacy Pathfinder include the following.

Potential Benefits of the APEC Data Privacy Pathfinder for Peru

- Create enhanced opportunities for cross-border business development; reduce trade barriers.
- Provide a competitive advantage for Peruvian industries seeking access to global supply chain networks.
- Enable SMEs in Peru to access global market opportunities.
- Assist Peru to address quickly possible commitments in the privacy domain to international organizations such as the OECD.
- Enable participation in a flexible framework for data privacy.
- Enhance data privacy protection for consumers/citizens involved in cross-border transactions.
- Explore capacity-building opportunities for implementation of the APEC Pathfinder.

Private Sector Considerations

- Numerous enterprises in Peru have already adopted strong information security and data privacy processes based on international best practices.
- Many businesses consider data privacy a requirement for doing business in today's digital economy.
- Those involved in SMEs, including hi-tech entrepreneurs seeking to access global market opportunities, are also aware of the need for data privacy practices and processes for cross-border transactions.
- Such businesses may have already built data privacy costs into their financial models.
- Regulatory impact may be small relative to the enhanced competitiveness that a data privacy regime can provide where the legal framework for data privacy is designed for efficiency and is based on internationally-accepted principles and best practices.
- Potential costs in terms of lost opportunities may be greater than costs associated with an effective data privacy legal infrastructure.

NEXT STEPS

This Report focuses on the legal and regulatory aspects of creating the appropriate legal infrastructure through which Peru can move forward with its efforts to implement the APEC Data Privacy Pathfinder and participate in the CBPR System as quickly as possible.

- Peru has demonstrated active participation in the APEC Data Privacy Pathfinder program.
- The economy has achieved legislative reform by enacting Law No. 29733–Law on Protection of Personal Data.
- It has designated one government entity–the Ministry of Justice–to lead the process of drafting the necessary modifications to Peruvian law to implement its legal infrastructure for privacy.
- It has drafted the proposed regulation to implement the Law on Protection of Personal Data and published it for public comment in September 2012

While the data protection law and proposed regulation include strong privacy protections, these provisions do not provide the legal authority for the APEC Data Privacy Framework or enable the establishment of an Accountability Agent and the Enforcement Authority in a manner that is fully compliant with the APEC Data Privacy Pathfinder. In order to move forward with its efforts to implement the APEC Data Privacy Pathfinder, and to meet its goal of being accepted as a participant in the CRPR System, Peru will need to review carefully the text of the proposed enabling regulation for the data protection law to ensure it includes those elements that will enable participation in the APEC Data Privacy Pathfinder and establishment of an Accountability Agent and implementation of the Enforcement Authority program.

Selection of the Accountability Agent Model

Each of the Accountability Agent models (public sector versus private sector) identified in the APEC Data Privacy Pathfinder was discussed during consultations in Peru. Given Peru's background, electronic commerce development, and overall regulatory approach, there appears to be a strong sentiment that the public sector model would be consistent with Peru's needs.

As noted above, the Law on Protection of Personal Data does not appear to address the government-centered Accountability Agent model directly. Peru's policy-makers may wish to consider where the official Accountability Agent function would be located within the government. It is possible, for example, that the function could be created under the regulatory powers of the new National Authority for Protection of Personal Data, or located in another part of The Ministry of Justice. Alternatively, it could be housed in a separate agency such as INDECOPI, which already has considerable dealings with the business and consumer communities. Further, there may be other agencies that could undertake the Accountability Agent functions. Since the proposed regulation does not explicitly create an Accountability Agent system under the regulatory powers provided to the National Authority, it will be important for Peruvian officials to determine whether an explicit authorization is required.

An Accountability Agent must be able to conduct, at appropriate intervals, ongoing compliance monitoring of the privacy notices and procedures of companies participating in the CBPR System. This includes reviewing privacy policies posted online, as well as privacy procedures followed at the points of collection of personal information. Peru officials should consider what is the best approach in light of the CBPR System requirements; the availability of technical solutions, for example, the use of web crawling software; whether it is feasible to accomplish the Accountability Agent functions using a manual review process; the costs involved; and Peru's goals and objectives. If many companies participate in the CBPR System, or large companies collect voluminous amounts of personal data online, it may be necessary to automate the review process.

Valuable information and feedback may be obtained from economies that have adopted various accountability agent models, including Chile, Vietnam, Japan, and the United States. It may also be helpful to review private sector Accountability Agent models and the work of the organizations that serve in that capacity.[31]

Implementation of the Enforcement Authority

In addition to selecting and implementing the Accountability Agent model under the Pathfinder program, a member-economy must designate the "Enforcement Authority." The Peru data protection law creates the new National Authority for Protection of Personal Data with responsibility assigned to the Ministry of Justice. The proposed regulation names the General Department of Personal Data Protection as the new office in charge of implementing the data protection law.

As next steps, after a decision is made concerning where to establish an Accountability Agent, it will then be necessary to develop policies and procedures for implementing the Accountability Agent functions. It is also critical to establish policies and procedures for the operation of the Enforcement Authority with primary legal responsibility for enforcing Peru's privacy laws affecting private sector entities consistent with the APEC Pathfinder Framework and the CBPR System.

Careful drafting of the regulation, directives and policies is required to achieve a legal framework that is compliant with the APEC Data Privacy Pathfinder and the APEC Privacy Framework. This should take into account not only domestic law but also standards established in other APEC member economies. These considerations should be included in the regulatory scheme to ensure that the legal structure will fully support the enforcement elements of the APEC Data Privacy Pathfinder program.

---

[31] Private sector Accountability Agents include the Better Business Bureau (BBB), Truste, and KPMG, to name just a few.

Completion of the draft Notice of Intent to Participate in the APEC CBPR System – Program Requirements and Enforcement Map

Peru has made significant progress in completing the APEC documents required to participate in the CBPR System. To participate in the CBPR System, an APEC member economy must accomplish these three steps:

> **Step 1:** Join the Cross-Border Privacy Enforcement Arrangement (CPEA)[32] (a voluntary network between regulators to facilitate cooperation on privacy-related investigations and enforcement action).
>
> **Step 2:** Submit a letter of intent to participate in the CBPR System.
>
> **Step 3:** Make use of at least one APEC-recognized Accountability Agent.[33]

In addition, the economy must provide:

1) A narrative description of the relevant domestic laws and regulations which may apply to any CBPR certification-related activities of an Accountability Agent operating within Peru's jurisdiction and the Enforcement Authority associated with these laws and regulations; and

2) The *APEC Cross-Border Privacy Rules System Program Requirements Enforcement Map* and additional narrative explanation of Peru's ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements.

The *APEC Cross-Border Privacy Rules System Program Requirements Enforcement Map* focuses on Peru's ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements. The enforcement map sets forth the baseline program requirements of the APEC CBPR System and provides an explanation of how each requirement may be enforced in Peru.

— Column 1 lists the questions in the intake questionnaire to be answered by an applicant organization when seeking CBPR certification. These are organized according to the APEC principles: preventing harm; notice; collection limitation; uses of personal information; choice; integrity; security safeguards; access and correction; and accountability.

— Column 2 lists the assessment criteria to be used by an APEC-recognized Accountability Agent when verifying the answers provided in Column 1.

---

[32] Membership currently includes agencies and ministries in the economies of Australia; New Zealand; United States; Hong Kong, China; Canada; and Japan.

[33] Accountability Agent APEC Recognition Application, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.ashx.

— Column 3 is completed by the Peruvian ECSG delegation or appropriate governmental representative and explains the enforceability of an applicant organization's answers in Column 1.

The APEC CBPR System Enforcement Map[34] looks like this:

Question (to be answered by Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy)
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)?	If YES, the Accountability Agent must verify that the privacy statement) include the following characteristics: [criteria are specified in the table]	Specify applicable laws and regulations; Describe enforcement mechanisms.
2….[A]t the time of collection of personal information… do you provide notice that such information is being collected?		
Continues with questions 3-50.		

Accountability Agents should be able to enforce the CBPR program requirements through law or contract. Peru's privacy Enforcement Authority should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements.

When completing the enforcement map, it is necessary to map each of the enforcement provisions of the data protection law and the proposed implementing regulation (summarized above) to the privacy requirements listed in column 1.

As described above, the proposed regulation for the data protection law (Title IV, Chapter III) creates a protection procedure for data subjects to pursue complaints against the holder of a database or data controller for alleged violations of privacy rights. Title VI specifies the violations that may be investigated and sanctions that may be imposed by the Department of Supervision and Control or the General Director of Personal Data Protection. The Director of Sanctions and the General Director of Personal Data Protection may pursue the application of sanctions under procedures in Title VI Chapter II and the sanctions specified in Chapter III.

[34] *See*, APEC Cross-Border Privacy Rules System Program Requirements: Enforcement Map, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-TemplateNoticeOfIntent.ashx.

Work Completed During the Capacity-Building Workshop

During the consultations in Peru, participants reviewed the template *Notice of Intent to Participate in the APEC CBPR System Program Requirements and Enforcement Map* and discussed the information that would be needed to complete all the forms.

Substantial time was devoted to completing a draft of the entire enforcement map. Participants identified the provisions of the data protection and related laws that pertain to each of the 50 questions in column 1, and they entered appropriate summaries in column 3.

In addition, participants prepared a summary of the framework that exists in Peru for enforcing the data protection law, including administrative procedures, and civil and criminal actions that may be pursued.

Next Steps for the Peru Ministry of Justice and ECSG Team

The final step to complete column 3 is to add a summary (such as the language proposed below modeled after the United States' privacy enforcement map) of the practices for each of the 50 questions that could constitute a violation of the data protection act. Peru officials who drafted the data protection law and the proposed implementing regulation have the expertise to adapt and tailor this language for each of the 50 questions and show how the applicable provisions of the law and regulations apply.

Completing Column 3–Suggested Language[35]

- The Ministry of Justice, through the National Authority for Protection of Personal Data, enforces Peru Law–29733 Protection of Personal Data (*Ley de Protección de Datos Personales*). This overarching privacy law provides broad private sector data privacy protection.

  A company that joins the APEC CBPR System must publicly declare that it will comply with the CBPR program requirements and must make these program requirements publicly accessible. If the company fails to comply with any of these program requirements, its public representation of compliance may constitute an unfair or deceptive act or practice subject to enforcement by The Ministry of Justice.
- If a company engages in any of the following practices it may violate the data protection act and be subject to an enforcement action:
  a. Making a public representation relating to the notice requirements and failing to comply with the representation;
  b. Displaying a seal, trustmark, or other symbol on the company's website or on any other of its own publicly available documentation that indicates that it participates in the APEC CBPR System and thus complies with the notice requirements and failing to comply; or
  c. Causing the company's name to appear on a list of companies that are certified for participation in the APEC CBPR System (e.g., lists on the websites of participating

[35] Modeled after the United States' privacy enforcement map. *See* http://ftc,gov/opa/2012/07/apec.shtm.

government authorities, privacy enforcement authorities, recognized APEC Accountability Agents, or on an APEC website specifically dedicated to the operation of APEC CBPR), thereby indicating that it complies with the notice requirements and failing to comply.

The Ministry of Justice has an established enforcement framework consisting of administrative procedures.

Title IV of the proposed regulation (Chapter III) creates a protection procedure for data subjects to pursue complaints against the holder of a database or data controller for alleged violations of privacy rights. Title VI specifies the violations that may be investigated and sanctions imposed. In addition, the regulation provides requirements for security and access control, and the authority to levy fines on both public and private organizations that do not provide appropriate levels of security for personal data.

Additional Recommendations

Following are a number of additional recommendations for consideration based on the review of the legal materials available at the time of the Peru Workshop as well as the very beneficial and open discussions held with representatives of The Ministry of Justice and the Ministry of Foreign Trade and Tourism (MINCETUR).

- Prepare an organizational strategy for government implementation of the APEC Data Privacy Pathfinder; develop agency expertise in the area of the APEC Privacy Framework and personal information/data privacy policy in general.

- Create and implement broad communications and educational programs that will effectively inform businesses of the benefits of the Accountability Agent program and raise the public's awareness of the importance of data privacy in the online environment and to build confidence in the Accountability Agent and Enforcement Authority programs.

- Consider ICT enhancements to create automated systems to reduce processing time in the work of an Accountability Agent and the Enforcement Authority, such as web crawling software or other automated approaches.

- Programs that enhance the "agency expertise," both legal and management, for operating the Accountability Agent program will be important. This will ensure consistency in decision-making processes, including those in the dispute resolution area, as well as for building confidence among business entities, online consumers, and others whose personal data may be subject to the Pathfinder Cross-Border Data Privacy Rules. Having this type of expertise will also provide consumers with the "trust" that will be central to the success of Peru's Accountability Agent program.

Appendix 1

Capacity-Building for CBPR Implementation in Peru–AGENDA

[Note: Meetings were held in Lima, Peru with representatives of The Ministry of Justice and the Ministry of Foreign Trade and Tourism (MINCETUR), August 13–14, 2012. Following is the Agenda for this capacity building Workshop.]

Monday, August 13, 2012

CROSS-BORDER PRIVACY ENFORCEMENT ARRANGEMENT – REQUIRED STEPS – LUCY THOMSON

1. Sources of "Privacy Law"
   - Constitution
   - Statutes and Laws
   - Presidential or Executives Decrees
   - Ministerial Decrees
   - Ministry Regulations
   - International Agreements or Treaties
   - Other?
2. Mechanics of Peru's Participation in the CBPR –
   How a Privacy Enforcement Authority Can Become a Participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA)
   - How to join the CPEA, a voluntary cooperation network between regulators
   - Submit a letter of intent to the CPEA Administrator to participate in the CBPR System
   - Confirm that the Privacy Enforcement (PE) Authority meets the definition of 'Privacy Enforcement Authority' set out in the CPEA
   - Submit a letter of confirmation from an appropriate government official verifying the PE Authority's status
   - Supply a contact point notification and a statement of its practices, policies, and activities

     [Template forms posted on the APEC Information Management Portal at http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce/cpea.html]
   - What happens if there is more than one Ministry responsible for Privacy Enforcement?
     [Handout – APEC Fact Sheet: APEC Cross-border Privacy Enforcement Arrangement]
3. Experiences with Safety Measures for Data Privacy Protection (Technical and Administrative Measures)
4. Treatment of Data in the Context of Cloud Computing (How do controls operate here?)
5. General Discussion (All Participants)

REVIEW OF PERU'S PRIVACY LAWS –PERU OFFICIALS

1. Constitution of Peru
2. Law on the Protection of Personal Data, No. 29733 (July 2, 2011)
    a. General Comments
    b. Sections from which the Data Protection Authority's powers could be established
3. Other laws, regulations, decrees, and policies
4. National Authority for the Protection of Personal Data
    a. Establishment
    b. Will other Ministries have a role in privacy enforcement?
    c. What are the mission and responsibilities of each Ministry for privacy protection?
5. What Ministry is authorized by law to sign the Cross-border Privacy Enforcement Arrangement (CPEA)?
6. Is enabling legislation required? What Regulations may be sufficient?

Tuesday, August 14, 2012

MAP PERU'S LAWS TO CBPR PROGRAM REQUIREMENTS –LUCY THOMSON AND PERU OFFICIALS

- Must be submitted in order to participate in the CBPR System
- Shows how implementation will tie back to the CBPR baseline program requirements

[References: Template Notice of Intent to Participate in the APEC Cross-border Privacy Rules System and Peru Privacy Individual Action Plan (2006)]

NEXT STEPS FOR THE PERU PE TO BECOME A PARTICIPANT IN THE CPEA – LUCY THOMSON AND PERU OFFICIALS

1. Developing a Plan to Sign the CPEA Agreement
2. Other Elements of the Pathfinder Program to be considered?
3. Developing the Final Report – Content and Issues
4. Follow-up Schedule

SUMMARY, CONCLUSIONS, AND FOLLOW-UP – LUCY THOMSON