



Data protection regulations and international data flows: Implications for trade and development





Data protection regulations and international data flows: Implications for trade and development



NOTE

Within the UNCTAD Division on Technology and Logistics, the ICT Analysis Section carries out policy-oriented analytical work on the development implications of information and communication technologies (ICTs). It is responsible for the preparation of the *Information Economy Report* as well thematic reports on ICT for development such as this study. The ICT Analysis Section promotes international dialogue on issues related to ICTs for development, and contributes to building developing countries' capacities to measure the information economy and to design and implement relevant policies and legal frameworks.

The E-Commerce and Law Reform Programme has supported developing countries in Africa, Asia and Latin America since 2000 in their efforts to establish legal regimes that address the issues raised by the electronic nature of ICTs to ensure trust in online transactions, ease the conduct of domestic and international trade online, and offer legal protection for users and providers of e-commerce and e-government services. UNCTAD helps to build the capacity of policymakers and lawmakers at national and regional levels in understanding the underlying issues underpinning e-commerce. The assistance targets, in particular, ministry officials in charge of law reform who need to learn more about the legal implications of ICTs; parliamentarians who have to examine new cyberlaws; and legal professionals who enforce new legislation.

The views presented in part II of the study are those of the contributors and do not necessarily reflect the views and position of the United Nations or the United Nations Conference on Trade and Development.

This publication has been edited externally.

The material contained in this study may be freely quoted with appropriate acknowledgement.

PREFACE

Increasingly, an ever-wider range of economic, political and social activities are moving online, encompassing various ICTs that are having a transformational impact on the way business is conducted, and the way people interact among themselves, as well as with government, enterprises and other stakeholders. This new landscape gives rise to new business models and a wider scope for innovation. At the same time, it facilitates undesirable activities online, including cybercrime. Against this background, world leaders in 2015 underscored the importance of adopting relevant policy responses to harness the potential of ICTs for all seventeen Sustainable Development Goals (SDGs).


Creating trust online is a fundamental challenge to ensuring that the opportunities emerging in the information economy can be fully leveraged. The handling of data is a central component in this context. In today's digital world, personal data are the fuel that drives much commercial activity online. However, how this data is used has raised concerns regarding privacy and the security of information.

The present regulatory environment on protection of data is far from ideal. In fact, some countries do not have rules at all. In other cases, the various pieces of legislation introduced are incompatible with each other. Increased reliance on cloud-computing solutions also raise questions about what jurisdictions apply in specific cases. Such lack of clarity creates uncertainty for consumers and businesses, limits the scope for cross-border exchange and stifles growth.

As the global economy shifts further into a connected information space, the relevance of data protection and the need for controlling privacy will further increase. Understanding different approaches to and potential avenues for establishing more compatible legal frameworks at national, regional and multilateral levels is important for facilitating international trade and online commerce. The rules surrounding data protection and cross-border flows of data affect individuals, businesses and governments alike, making it essential to find approaches that address the concerns of all stakeholders in a balanced manner.

This study is a timely contribution to our understanding of how data protection regulations and international data flows affect international trade. It reviews the experience in different parts of the world and of different stakeholders. The study identifies key concerns that data protection and privacy legislation need to address. It also examines the present patchwork of global, regional and national frameworks to seek common ground and identify areas where different approaches tend to diverge. The last part of the study considers possible future policy options, taking the concerns of all stakeholders into account.

I would like to acknowledge with appreciation the valuable contributions received from various stakeholders. I hope that the findings presented will serve as a basis for a much-needed global dialogue aimed at building consensus in a very important policy field.



Taffere Tesfachew
Acting Director, Division on Technology and Logistics

April 2016

ACKNOWLEDGEMENTS

The study on Data Protection Regulations and International Data Flows: Implications for Trade and Development was prepared by a team comprising Torbjörn Fredriksson (team leader), Cécile Barayre and Olivier Sinoncelli. Chris Connolly was the lead consultant for the study.

Because data protection is a global issue, it was important for UNCTAD to consult with a wide range of stakeholders to identify their concerns and issues they face. UNCTAD would like to thank all those countries and organizations that contributed inputs for the study: Adjaïgbe S. Rodolphe (Benin), Rafael Zanatta (Brazilian Institute of Consumer), Denis Kibirige and Barbarah Imaryo (Uganda), Danièle Chatelois (Asia-Pacific Economic Cooperation), Elizabeth Bakibinga-Gaswaga (Commonwealth Secretariat), Atte Boeyi and Ado Salifou Mahamane Laoualy (Niger), Robert Achieng (East African Community), Liz Coll and Richard Bates (Consumers International), Joseph Alhadeff (International Chamber of Commerce), Raphael Koffi and Isaias Barreto Da Rosa (Economic Community Of West African States), Maria Michaelidou (Council of Europe), Lukasz Rozanski (European Commission), Moctar Yedaly, Amazouz Souhila and Auguste K. Yankey (African Union Commission), Albert Antwi-Boasiako (e-Crime Bureau, Ghana), Bijan Madhani and Jordan Harriman (Computer and Communications Industry Association), Melinda Claybaugh and Hugh Stevenson (United States Federal Trade Commission) and Ammar Oozeer (Mauritius). Additional substantive inputs were provided by Eduardo Ustaran (International Association of Privacy Professionals), Olanrewaju Fagbohun (Nigerian Institute of Advanced Legal Studies), Yasin Beceni (BTS & Partners), Ussal Sahbaz (Economic Policy Research Foundation of Turkey), Geff Brown, Marie Charlotte Roques Bonnet, Ed Britan and Heba Ramzy (Microsoft).

Comments on a draft version of the study were provided by Anupam Chander, Graham Greenleaf and Ian Walden. The data shared by Galexia for this study is greatly appreciated.

The cover was prepared by Nadège Hadjemian. Desktop publishing was completed by Ion Dinca. The document was edited by Nancy Biersteker.

Financial support from the Governments of Finland and the Republic of Korea is greatly appreciated.

CONTENTS

PART I	1
Executive Summary.....	xi
Introduction.....	1
Objectives of this study	1
The growing importance of data protection.....	1
Trade implications of data protection	3
Outline of this study	4
CHAPTER I KEY CHALLENGES IN THE DEVELOPMENT AND IMPLEMENTATION OF DATA PROTECTION LAWS	7
A. Addressing gaps in coverage.....	8
B. Addressing new technologies.....	10
C. Managing cross-border data transfers	12
D. Balancing surveillance and data protection	15
E. Strengthening enforcement	16
F. Determining jurisdiction	18
G. Managing the compliance burden for business.....	20
CHAPTER II GLOBAL DEVELOPMENTS AND LESSONS LEARNED	23
A. The United Nations	24
B. The Council of Europe Convention 108.....	25
C. The OECD	26
D. International Data Protection Commissioner's initiatives.....	27
Lessons learned from the global initiatives	27
CHAPTER III REGIONAL INITIATIVES	31
A. The European Union (EU)	32
B. Asia-Pacific Economic Cooperation (APEC)	34
C. African Union (AU).....	35
D. The Commonwealth.....	35
E. Trade agreements	36
Lessons learned from the regional initiatives.....	37
CHAPTER IV SELECT NATIONAL INITIATIVES AND EXPERIENCES	41
Country snapshots	43
Lessons learned from national data protection laws.....	47
CHAPTER V PRIVATE SECTOR AND CIVIL SOCIETY PERSPECTIVES	49
A. The private sector	50
B. Civil society.....	51
CHAPTER VI CONCLUSIONS	55
CHAPTER VII POLICY OPTIONS	60

Policy options for international and regional organizations.....	62
Policy options for countries.....	64
Part II	69
International and Regional Organizations	71
Private Sector and NGOs	95
Governments.....	115

International and Regional Organizations

African Union Convention on Cyber-security and Personal Data Protection (AU CCPDP). Moctar Yedaly, Head, Information Society Division, Infrastructure and Energy Department, AU Commission.

Privacy Policy Developments in the Asia Pacific Economic Cooperation (APEC) Forum. Danièle Chatelois, Former Chair of the APEC Data Privacy Subgroup (2012-February 2016).

Data Protection in the Commonwealth. Elizabeth Bakibinga-Gaswaga, Legal Advisor, International Development Law, Commonwealth Secretariat.

The Council of Europe Convention 108. Maria Michaelidou, Programme Advisor, Data Protection Unit, Council of Europe.

Data Protection in the East African Community. Robert Achieng, Senior Communications Engineer, EAC Secretariat.

ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection. Dr. Isias Barreto Da Rosa, Commissioner for Telecommunication and Information Technologies, ECOWAS Commission.

Data Protection in the European Union: Today and Tomorrow. Lukasz Rozanski, European Commission.

Private Sector and NGOs

Personal Data Protection and International Data Flows: The Case of Brazil. Rafael Zanatta, Brazilian Institute of Consumer.

Cross-border e-commerce: building consumer trust in international data flows. Liz Coll, Consumers International.

Comments of the Computer & Communications Industry Association on Data Protection Regulations and International Data Flows: Impact on Enterprises and Consumers. Bijan Madhani, Public Policy & Regulatory Counsel; Jordan Harriman, Policy Fellow, CCIA.

Optimizing Societal Benefit of Emerging Technologies in Policy Development Related to Data Flows, Data Protection and Trade. Joseph Alhadeff, Chair, International Chamber of Commerce Commission on the Digital Economy; Chief Privacy Strategist and Vice President of Global Public Policy, Oracle Corporation.

Middle East and Africa (MEA) Privacy Principles Will Protect Privacy and Advance Trade, The Case for a New Legal Framework. Eduardo Ustaran, IAPP board member, Olanrewaju Fagbohun, Research Professor, Nigerian Institute of Advanced Legal Studies, Yasin Beceni, Managing Partner, BTS & Partners; and Lecturer; Istanbul Bilgi University, Ussal Sahbaz, Director, Think Tank – TEPAV, Geff Brown, Assistant General Counsel, Microsoft Corp., Marie Charlotte Roques Bonnet, Director Microsoft EMEA, Ed Britan, Attorney, Microsoft Corp., Heba Ramzy, Director Corporate Affairs, Microsoft Middle East and Africa.

Governments

The Protection of Data in Benin. Adjaigbe S. Rodolphe, Director, Studies and Research, Ministry of Communication and ICTs, Benin.

Implementation of Data Protection Legislation - The Case of Ghana. Albert Antwi-Boasiako, Founder and Principal Consultant, e-Crime Bureau, Ghana.

The Status of Data Protection in Mauritius. Ammar Oozeer, Juristconsult Chambers, Mauritius.

The Status of Data Protection in Niger. Atte Boeyi, Director of Legislation, General Secretariat; Ado Salifou Mahamane Laoualy, Director of Judicial Affairs and Litigation, Niger.

The Legal and Regulatory Regime for Data Protection and Privacy in Uganda. Denis Kibirige, Senior State Attorney, Ministry of Justice and Constitutional Affairs (MoJCA); Barbarah Imaryo, Manager, Legal Services, National Information Technology Authority (NITA-U), Uganda.

Privacy and Security of Personal Data in the United States. Staff of the Federal Trade Commission Office of International Affairs, United States.

Boxes

Box 1:	Schrems v Facebook (Ireland, Europe, 2014/2015)	15
Box 2:	Office of the Privacy Commissioner for Personal Data v Octopus (Hong Kong, 2010)	17
Box 3:	The Benesse data breach (Japan, 2014)	17
Box 4:	FTC v TRUSTe (United States, 2015)	17
Box 5:	US v Microsoft (2014-2015, United States)	18
Box 6:	FTC v Accusearch (2009, United States)	18
Box 7:	Belgian Commission for the Protection of Privacy v Facebook (Belgium, 2015/2016)	19
Box 8:	Summary of revisions made to the 1980 OECD Privacy Guidelines in 2013	26

Tables

Table 1.	Strengths and limitations of the various approaches to ongoing exceptions	14
Table 2.	Strengths and limitations of the main global initiatives in addressing key challenges in the development and implementation of data protection laws	28
Table 3.	Strengths and limitations of the main regional frameworks in addressing key challenges in the development and implementation of data protection laws	38
Table 4.	Summary of the main findings on key challenges in the development and implementation of data protection laws	58

Figures

Figure 1:	Challenges faced by ASEAN countries and selected countries in the ECOWAS, Latin America and the Caribbean (48 countries) in enacting data protection legislation.	8
Figure 2:	Challenges faced by ASEAN countries and selected countries in the ECOWAS, Latin America and the Caribbean (48 countries) in enforcing data protection legislation.	9
Figure 3:	Data Protection and the Digital Economy	11
Figure 4:	Global percentage of comprehensive, partial/sectoral and draft data protection laws in each region	42
Figure 5:	Data Protection Core Principles	57
Figure 6:	Key Policy Options	62

LIST OF ABBREVIATIONS

APEC:	Asia Pacific Economic Cooperation
APPI (Japan):	Act for Protection of Personal Information
ASEAN:	Association of Southeast Asian Nations
AU:	African Union
AU CCPDP:	African Union Convention on Cyber-security and Personal Data Protection
B2C:	business-to-customer (or business-to-consumer)
BC:	Budapest Convention
BCRs (EU):	Binding Corporate Rules system
BPO:	Business process outsourcing
C2C:	customer-to-customer (or consumer-to-consumer)
CAN-SPAM :	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 Act (U.S.)
CBPR system or CBPRS (APEC):	Cross-Border Privacy Rules System
CEMAC:	Communauté Économique et Monétaire de l’Afrique Centrale
CERTs/CSIRTs:	Computer Emergency Response Teams
CFPB (U.S.):	Consumer Financial Protection Bureau
CHOGM:	Commonwealth Heads of Government Meeting
CHRAJ (Ghana):	Commission on Human Rights and Administrative Justice
CIPL:	Centre for Information Policy Leadership
CIPPIC:	Canadian Internet Policy and Public Interest Clinic
CJEU:	Court of Justice of the European Union
CNIL (France):	Commission nationale de l’informatique et des libertés (National Commission on Computer Science and Freedoms)
CoE:	Council of Europe
COPPA (U.S.):	The Children’s Online Privacy Protection Act
CPEA (APEC):	Cross-Border Privacy Enforcement Arrangement
CSP:	Customer Service Providers
DPA (Mauritius):	Data Protection Act
DPC (Ghana):	Data Protection Commission
DPS (APEC):	Data Privacy Subgroup
ECCAS:	Economic Community of Central African States
ECIPE:	European Centre for International Political Economy
ECOWAS:	Economic Community of West African States
ECSG:	Electronic Commerce Steering Group
EM:	Emerging Markets
EMEA (Microsoft):	<i>Europe, the Middle East and Africa</i>
eT:	e-transactions
FCC (U.S.):	Federal Communications Commission
FCRA (U.S.):	The Fair Credit Reporting Act
FERPA (U.S.):	Family Educational and Privacy Rights Act
FGV (Law School):	Fundação Getulio Vargas
FIPPs (U.S.):	Fair Information Practice Principles
FTC (U.S.):	Federal Trade Commission
GATS:	The General Agreement on Trade in Services

GDPR (EU):	General Data Protection Regulation
GLB Act (U.S.):	Gramm-Leach-Bliley Act
GPEN:	Global Privacy Enforcement Network
HHS (U.S.):	Department of Health and Human Services
HIPAA (U.S.):	The Health Insurance Portability and Accountability Act of 1996
IAPP:	<i>International Association of Privacy Professionals</i>
ICO (UK):	Information Commissioner's Office
IDEC:	Instituto Brasileiro de Defesa do Consumidor (Brazilian Institute of Consumer)
IDPC:	International Data Protection Commissioners
IoE:	Internet of Everything
IoT:	Internet of Things
ITES:	Information Technology Enabled Service
ITI:	Information Technology Industry Council - (note: U.S.-based)
ITU:	International Telecommunications Union
JRA (U.S.):	Judicial Redress Act
LAP:	London Action Plan International Cybersecurity Enforcement Network
MDAs (Ghana):	Ministries, Departments and Agencies
MoICT (Uganda):	Ministry of Information and Communications Technology
MoJCA (Uganda):	Ministry of Justice and Constitutional Affairs
NCA (Ghana):	National Communication Authority
NITA (Ghana):	National Information Technology Agency
NITA-U (Uganda):	National Information Technology Authority
ODR:	Online dispute resolution
OECD:	Organisation for Economic Cooperation and Development
OPC (Canada):	Office of the Privacy Commissioner
PDP:	Personal data protection
PDPA (Singapore):	Personal Data Protection Act
PEA:	Privacy Enforcement Authority
PICO (Korea):	Personal Information Dispute Mediation Committee
PIPC	
(Japan and Korea):	Personal Information Protection Commission
PIPEDA (Canada):	Personal Information Protection and Electronic Documents Act
PRP (APEC):	Privacy Recognition for Processors System
RECs:	Regional Economic Communities
SADC:	Southern African Development Community
SCA (U.S.):	Stored Communications Act
SCCs:	Standard Contractual Clauses
SIIA (U.S.):	Software & Information Industry Association
SMEs:	Small and medium enterprises
TEPAV:	Economic Policy Research Foundation of Turkey
TFEU (EU):	Treaty on the Functioning of the European Union
TiSA:	Trade in Services Agreement
TPP:	Trans-Pacific Partnership
TTIP:	Transatlantic Trade and Investment Partnership
UBPOA:	Uganda Business Process Outsourcing Association
UNECA:	United Nations Economic Commission for Africa
UNGCP:	United Nations Guidelines on Consumer Protection
VoIP:	Voice over Internet Protocol
WAEMU:	West African Economic and Monetary Union

EXECUTIVE SUMMARY

In the global information economy, personal data have become the fuel driving much of current online activity. Every day, vast amounts of information are transmitted, stored and collected across the globe, enabled by massive improvements in computing and communication power. In developing countries, online social, economic and financial activities have been facilitated through mobile phone uptake and greater Internet connectivity. As more and more economic and social activities move online, the importance of data protection and privacy is increasingly recognized, not least in the context of international trade. At the same time, the current system for data protection is highly fragmented, with diverging global, regional and national regulatory approaches.

This study reviews the current landscape and analyzes possible options for making data protection policies internationally more compatible. It also provides a fresh and balanced take on related issues by considering the varied perspectives of different stakeholders. Written contributions from key international organizations, government bodies, the private sector and civil society offer valuable insight into the current state of affairs.

The findings of the study should help to inform the much needed multi-stakeholder dialogue on how to enhance international compatibility in the protection of data and privacy, especially in relation to international trade, and to provide policy options for countries that wish to implement new laws or amend existing ones. The study will serve as a basis for deliberation during the UNCTAD E-Commerce Week and for its capacity-building activities related to E-Commerce and Law Reform.

Importance of data protection and privacy laws

Data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of utmost importance for global trade flows that increasingly rely on the Internet.

Many social and cultural norms around the world include a respect for privacy. While underlying privacy principles contain many commonalities across countries, interpretations and applications in specific jurisdictions differ significantly. Some protect privacy as a fundamental right, while others base the protection of individual privacy in other constitutional doctrines or in tort. Still others have yet to adopt privacy protections. Such differences will increasingly affect individuals, businesses and international trade.

The information economy is increasingly prominent and promises to provide many opportunities, but could also generate some potential drawbacks. Internationally compatible data protection regimes are desirable as a way to create an environment that is more predictable for all stakeholders involved in the information economy and to build trust online.

New technological developments are adding urgency to this need. Cloud computing has quickly risen to prominence, disturbing traditional models in various areas of law, business and society. Certain projections estimate that the cloud computing industry will have a projected global market worth of \$107 to \$127 billion by 2017.¹ The Internet of Things is also rapidly developing, and has a direct nexus to management of data. While forecast reports vary greatly, one report estimates that value-added services related to the Internet of Things will grow from around \$50 billion in 2012 to approximately \$120 billion in 2018, and that there will be between 20-50 billion connected devices by 2020.² Another report forecasts a potential economic impact of between \$3.9 and \$11.1 trillion per year in 2025.³

Data protection regulation must carefully correspond to the evolving needs and possibilities associated with these changes in order to facilitate potential benefits. In 2014, approximately \$30 trillion worth of goods, services and finance was transferred across borders. Around 12 percent of international trade in goods has been estimated to occur through global e-commerce platforms like Alibaba and Amazon. The international dimension of flows has increased global GDP by approximately 10 percent, equivalent to a value of \$7.8 trillion in 2014. Data flows represent an estimated \$2.8 trillion of this added value.⁴

Key Concerns

As the contributions to this study demonstrate, concerns related to data protection and privacy online manifest themselves in many different dimensions.

Governments - specifically in those developing countries attempting to adopt data protection legislation - are having problems modeling their data protection regimes, though most opt for an approach consistent with the EU Directive. Common challenges include (1) the length of time it takes to pass legislation, (2) financial costs associated with implementing and enforcing a data protection regime, and (3) a lack of public and private sector knowledge and cooperation among governmental entities regulating in parallel. In some countries, a lack of understanding and fear within society can also exacerbate one or more of the aforementioned difficulties.

On the consumer side, concerns related to payment system integrity, hidden costs, fear of fraud and product quality are often more pronounced in the context of international e-commerce. Building trust in the online environment is key, and there has been a decline in trust with regards to transactions with both government and private actors. Studies show that consumers are concerned about how their personal data are collected and used, and that these concerns are increasing. A lack of clarity with regard to protection and avenues for redress tends to further aggravate these concerns.

Businesses are concerned that (1) too stringent protection regimes will unduly restrict activities, increase administrative burdens and stifle innovation; (2) a lack of clarity and compatibility between regimes add uncertainty, with negative effects on investments; and (3) given the nexus between cross-border e-commerce and data protection, divergent regimes will inhibit the adoption and proliferation of emerging technological developments, reducing potential accompanying societal benefits.

Key messages

Although there is significant divergence in the detailed data protection laws of the world, there is more common ground around the core set of data protection principles that are said to be at the heart of most national laws and international regimes. This set of core principles can serve as a useful starting point for efforts towards achieving more compatibility and harmonization.

There is no single agreed model for data protection law at this stage. However, compatibility is the stated objective of many global and regional data protection initiatives.

Numerous challenges in the development and implementation of data protection laws exist. This study concentrates on seven areas where action is particularly needed.

1. Addressing gaps in coverage
2. Addressing new technologies
3. Managing cross-border data transfers
4. Balancing surveillance and data protection
5. Strengthening enforcement
6. Determining jurisdiction
7. Managing the compliance burden

Policy options for developing and implementing national laws

The number of national data protection laws has grown rapidly, but major gaps persist. Some countries have no laws in this area, some have partial laws, and some have laws that are outdated and require amendments. The study includes key policy options for nations that are developing, reviewing or amending their data protection laws.

For those countries that still do not have relevant laws in place, governments should develop legislation that should cover data held by the government and the private sector and remove exemptions to achieve greater coverage. A core set of principles appears in the vast majority of national data protection laws and in global and regional initiatives. Adopting this core set of principles enhances international compatibility, while still allowing some flexibility in domestic implementation.

Strong support exists for establishing a single central regulator when possible, with a combination of oversight and complaints management functions and powers. Moreover, the trend is towards broadening enforcement powers, as well as increasing the size and range of fines and sanctions in data protection.

Addressing the issue of cross-border data transfers using specific text and promoting one or more mechanisms that businesses can use to enable international data flows is crucial. In an increasingly globalized economy where more and more economic activities are undertaken online, remaining silent on

the issue is not a viable option. Allowing a range of options for companies to consider appears to be the accepted, modern approach to managing this issue.

National data protection laws should avoid (or remove) clear obstacles to trade and innovation. This may involve avoiding or removing data localization requirements that go beyond the basic options for the management of cross border data transfers. A useful test that has emerged in this area is the requirement that such provisions should not be 'disguised restrictions on trade'.

It is also increasingly difficult to ignore the need to balance government surveillance requirements against data protection. In some jurisdictions, data protection laws will be the appropriate place to address this issue. In others, it may be addressed through different legal arrangements. Countries need to implement measures that place appropriate limits and conditions on surveillance.

Policy options for global and regional data protection initiatives

The study discusses key policy areas for global and regional groups that play a role in data protection.

In order to promote international compatibility, it is important to avoid duplication and fragmentation in the regional and international approaches to data protection. It would be preferable for global and regional organizations to, instead of pursuing multiple initiatives, concentrate on one unifying initiative or a smaller number of initiatives that are internationally compatible. Where possible, similarities in underlying principles can be leveraged to develop mechanisms for recognition and compatibility between different frameworks.

Future work towards achieving greater compatibility will require the effective involvement of all stakeholders, including government, private sector and civil society representatives. Their involvement needs to go beyond general discussions to include formal engagement in the policy development process. This active involvement will also help develop measures that promote a higher level of certainty and confidence amongst stakeholders, which will increase the overall efficiency of legal frameworks.

The study includes some detailed guidance on the growing consensus around key conditions and limitations on surveillance initiated by governments. Most regional and global initiatives are silent on the issue of surveillance. It is essential that national laws and global and regional initiatives acknowledge the existence of surveillance issues and attempt to address these issues directly. While surveillance issues often have an international or cross-border dimension, the extraterritorial nature of data flows and surveillance, as it relates to state sovereignty, must be specifically addressed. The United Nations statement on digital rights may serve as a platform for considering the connection between data protection and surveillance.

In developing and promoting international and regional initiatives on data protection, consideration should also be given to the compliance burden, and the potential for negative impacts on trade, innovation and competition, especially from the perspective of SMEs. In this context, SMEs should be consulted and participate in debates related to such initiatives. Finally, prioritizing provisions that build consumer trust and confidence in regulatory models will help grow e-commerce activity.

Developing efficient policies across the globe is of utmost importance, especially with the advent of recent technological advances. Policies should strive to balance various legitimate stakeholder concerns while also carefully avoid solutions that will overly restrict trade. Getting the balance wrong can have serious consequences for either the protection of fundamental rights or for international trade and development. The study provides various examples of good practices that can be built upon.

Striving for balanced, flexible, and compatible data protection regulation has become an urgent goal. Some countries have powerful regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that allows for innovation and facilitates trade, it is essential to continue national, regional and global multi-stakeholder dialogue. International organizations dealing with trade and development, such as UNCTAD, can provide the platform for such dialogue.

NOTES

- ¹ See “2015 Top Markets Report: Cloud Computing.” U.S. Department of Commerce. International Trade Administration, July 2015. http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf. See also <http://openviewpartners.com/news/global-cloud-computing-services-market-to-reach-us127-billion-by-2017-according-to-new-report-by-global-industry-analysts-inc/>.
 - ² See “The Internet of Things: “Smart” Products Demand a Smart Strategy Using M&A for a Competitive Edge.” Woodside Capital Partners, March 2015. http://www.woodsidecap.com/wp-content/uploads/2015/03/WCP-IOT-M_and_A-REPORT-2015-3.pdf.
 - ³ See “The Internet of Things: Mapping the Value Beyond the Hype.” McKinsey Global Institute. June 2015. <http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.
 - ⁴ See “Digital Globalization: The New Era of Global Flows.” McKinsey Global Institute, March 2016. <http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.
-

PART I



INTRODUCTION

Objectives of this study

In the global information economy, personal data have become the fuel driving much of current online activity. Every day, vast amounts of information are transmitted, stored and collected across the globe enabled by massive improvements in computing and communication power. Some broadband packages of today are 36,000 times faster than what dial-up Internet connections could offer when the first Internet browser was introduced two decades ago. In developing countries, on-line social, economic and financial activities have been facilitated through mobile phone uptake and greater Internet connectivity. The transborder nature of the Internet as well as the speed and sheer volume of communications pose problems to cybersecurity such as those related to the identification, investigation, jurisdiction, criminalization and prosecution of those who commit security and data breaches. In this environment, security of information is a concern for governments, businesses and consumers alike.

Protecting data and privacy rights online is a significant and increasingly urgent challenge for policymakers.

Control over the information generated by online activities, and the access to it, is of concern to policymakers and legislators tasked with protecting their citizens from interference and harm. Analyses of 'big data' aimed at understanding and influencing consumer behaviour for commercial profit may further exacerbate such concerns.

From a trade perspective, transfers of data to and from developing countries may be inhibited by an absence of domestic legal protection, with missed business opportunities as a possible result. In countries that see exports of ICT-enabled services as a promising growth sector, data protection laws are important to comply with requirements in the importing countries. However, a majority of developing countries still lack legal frameworks to secure the protection of data and privacy.

The scope of definitions of personal data differs (broad or narrow) depending on the jurisdictions and data protection laws vary from country to country (and region to region). Their trade implications are not immediately clear for businesses, consumers and investors. This study aims to present the different regimes, their strengths and limitations and examines some of the

key dimensions of the current 'data protection and privacy' debates. The study discusses potential implications for cross-border trade of the various and sometimes divergent regulatory approaches that result in uneven levels of protection between jurisdictions. It also explores possible remedies by considering various options for implementing a robust data protection strategy.

The growing importance of data protection

Data protection laws date back to the 1970s, reflecting concerns about the emergence of computer and communication technologies, with their ability to process remotely large volumes of data. While numerous national, regional and international initiatives have pursued starkly different regulatory approaches, a remarkable degree of harmonization and coherence around the core principles that underpin them exists, as discussed below.

Common principles include the need to have a legitimate reason for any processing activity, obtained either through consent or some other justification designed to acknowledge competing private and public interests. The obligations concerning the quality of the personal data being processed is another core principle, requiring that data are accurate, complete and kept up-to-date. Compliance with this principle should be mutually beneficial to both the subject of the processing and the processor.

The role of data security is fundamental. Whether physical, logical or organizational, security measures should protect against deliberate acts of misuse, as well as the accidental loss or destruction of data. Similar to issues of data quality, implementing appropriate data security should combine the needs of individual data subjects, the entity processing the personal data and, indeed, society at large. Policymakers increasingly recognize the Internet as both a 'critical national infrastructure', over which an increasing proportion of daily economic and social activities is carried out, and as a source of vulnerability and threat. Addressing this duality and putting in place adequate data security measures should be a core component of the policy response.

While broad agreement exists on the basic principles, there is no consensus on how best to apply them. Some data protection regimes apply equally to all those processing personal data. Other regimes apply different rules to specified sectors (e.g. health), types of

processing entity (e.g. public authorities) or categories of data (e.g. data about children). In such jurisdictions, some sectors are not subject to regulatory controls at all.

A distinction can also be made between regimes that operate primarily through enforcement actions brought by individuals or their representative groups, and those that grant enforcement powers to a specialized supervisory authority, which exercises ongoing oversight over the conduct of those that process personal data. Some regimes operate through a combination of both approaches.

Data protection is recognized as an important field of law, policy development and regulation. It combines elements of human rights and consumer protection and, in many international agreements and individual jurisdictions, data protection is considered a fundamental right. At the same time, data protection regulation is also seen by many stakeholders as an enabling law, which facilitates the development of new technologies and innovations, and the promotion of international trade and development.

Data protection regulation is high on the political agenda at the time of writing, as evidenced by a number of current developments.

- The United Nations in 2015 appointed a Special Rapporteur on the right to privacy.⁵
- The European Union is finalizing a new General Data Protection Regulation to replace the European Directive on Data Protection, which has been a prominent source of regulation for twenty years.
- Data protection has been included in several international trade agreements.
- Data protection regulation has been considered in several high profile court cases in relation to national surveillance issues.
- Numerous countries are drafting new data protection laws or are reviewing existing ones.
- The European Union and the United States have re-negotiated a long standing cross-border data protection agreement (the former EU-US Safe Harbor Framework, now to be known as the EU-US Privacy Shield).
- Several global and regional organizations have issued (or are developing) multiparty agreements and/or guidelines on data protection.

Relevant initiatives are discussed in further detail in this study.

Trade implications of data protection

Divergent regulatory approaches result in uneven levels of protection between jurisdictions. This, in turn, leads to the need for legal controls over cross-border flows of personal data between jurisdictions, in order to prevent the laws of the more protective regime from being circumvented and the privacy rights of the individuals being eroded.

Article XIV (c) (ii) of the WTO's General Agreement on Trade in Services (GATS) permits trade restrictions that are necessary for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts", specifying that "such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services".

This is a very high level provision that recognizes the positive aspects of data protection regulation. However, it is also well recognized that if data protection regulations go 'too far' they may have a negative impact on trade, innovation and competition.

While the potential need to control cross-border flows of data for privacy purposes is clear, the application of such controls in an increasingly interconnected world is very challenging. ICT developments, such as cloud services, are making things even more complex, with processing entities not necessarily aware about where data are located. Although the answer may eventually be a technological one, increased harmonization of laws and regimes would greatly reduce the likelihood of friction over cross-border data flows.

Data protection is an increasingly important field, mostly due to the expansion of the digital/information economy. As more business models and practices move onto the digital platform and data becomes increasingly shared and exchanged on an international scale, its relationship to international trade intensifies. Since data are gathered, digitized, stored, and moved on a truly global basis by a multitude of parties, restrictions and regulations concerning data directly effect on global trade.

The Computer and Communications Industry Association (CCIA) summarizes the impact of data protection on digital trade as follows:

With the growth of digital flows and e-commerce have come concerns about the protection of personal data, and the security of digital transactions and content. These concerns are not just shared by consumers. Protection of data is at the core of the Internet's sustained growth as a platform for expression and trade in goods and services. In fact, the lifeblood of Internet-based industry—which today has grown to include a substantial component of all industries—is the trust that global Internet users have in online platforms.⁶

In recent years a number of studies have been published that highlight the scale and importance of cross-border data flows. The key findings include:

- Business to Business (B2B) e-commerce was estimated to be worth \$15 trillion in 2013. Business to Consumer (B2C) e-commerce was much smaller, at around \$1.2 trillion in 2013, but it was growing fast, especially in developing countries. China has already emerged as the world's largest single B2C e-commerce market;⁷
- in 2012, the United States exported \$140.6 billion worth of digitally deliverable services to the EU and imported \$86.3 billion worth of such services. In 2011, the supply of digitally deliverable services through U.S. affiliates in Europe was worth \$312 billion, while Europe supplied \$215 billion worth of digitally deliverable services through U.S. affiliates;⁸
- U.S. exports globally of digitally deliverable services in 2012 were \$383.7 billion and imports were \$233.6 billion. This represented 61 percent of total U.S. services exports and 53 percent of services imports. EU exports of digitally deliverable services in 2012 were \$465 billion and imports were \$297 billion globally;⁹ and
- in 2014, approximately \$30 trillion worth of goods, services and finance was transferred across borders. Around 12 percent of international trade in goods has been estimated to occur through global e-commerce platforms like Alibaba and Amazon. The international dimension of flows has increased global GDP by approximately 10 percent, equivalent to a value of \$7.8 trillion in 2014. Data flows represent an estimated \$2.8 trillion of this added value.¹⁰

Several studies have tried to estimate the potential impacts of data protection requirements that place unreasonable burdens on businesses or disrupt cross-border data transfers. Findings include:

- proposed economy-wide data localization requirements would lead to a negative impact on GDP in several countries where such requirements have been considered (Brazil -0.8%, India -0.8% and Republic of Korea -1.1%) or implemented (Indonesia -0.7%);¹¹
- for many countries that are considering forced data localization laws, local companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders;¹² and
- if services trade and cross-border data flows are seriously disrupted (between the EU and U.S.), the negative impact on EU GDP could reach -0.8% to -1.3%.¹³

Data protection is also important for facilitating the growth of the Business Process Outsourcing (BPO) and Information Technology Enabled Service (ITES) sectors. These are important industries, especially in developing nations, but they can only succeed if personal data can be transferred to the processing jurisdiction with trust and confidence that the data will be protected. Countries hoping to develop these industry sectors have a strong interest in data protection law. For example, Mauritius is seeking to have its data protection law recognized internationally by joining the Council of Europe Convention 108.¹⁴ Many other countries with growing BPO and ITES sectors have worked hard to establish strong data protection laws that meet international standards (for example, the Philippines and South Africa).

Outline of this study

This study has the following structure:

Part I

Chapter 1 discusses key challenges in the development and implementation of data protection laws. There are numerous challenges, but this study concentrates on seven key areas where action is needed.

Chapter 2 discusses four global data protection initiatives and the lessons learned from these.

Chapter 3 discusses four key regional data protection initiatives and also the impact of trade agreements on data protection.

Chapter 4 discusses select national initiatives and the lessons from the development and implementation of national data protection laws.

Chapter 5 discusses civil society and private sector perspectives on data protection.

Chapter 6 discusses the overall lessons and conclusions from the study.

Chapter 7 discusses potential policy options for global, regional and national stakeholders.

Part II

This part of the study presents contributions from various international and regional organizations, governments, the private sector and civil society. Each stakeholder has prepared a unique input, sharing their insights, experiences, challenges and ideas on promoting best practices in the area of data protection and privacy in the context of international trade. The contributions are organized under the following three headings: international and regional organizations, private sector and non-governmental organizations, and governments.

NOTES

⁵ <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

⁶ See the contribution of CCIA in Part II.

⁷ United Nations Conference on Trade and Development (UNCTAD), *Information Economy Study 2015 - Unlocking the Potential of E-commerce for Developing countries* (2015), http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf. The study notes that most e-commerce is domestic, but international e-commerce is growing rapidly.

⁸ Information Technology Industry Council, *The EU-U.S. Privacy Shield: What's at Stake* (2016), <http://www.itic.org/dotAsset/9/b/9b4cb3ad-6d8b-469d-bd03-b2e52d7a0ecd.pdf>

⁹ Brookings Institute, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* (2014), <http://www.brookings.edu/~media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf>

¹⁰ See "Digital Globalization: The New Era of Global Flows." McKinsey Global Institute, March 2016. <http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>

¹¹ European Centre for International Political Economy (ECIPE), *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

¹² Leviathan Security Group, *Quantifying the Cost of Forced Localization* (2015)

¹³ European Centre for International Political Economy (ECIPE) for the U.S. Chamber of Commerce, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

¹⁴ For further details, see the contribution of Mauritius in Part II

CHAPTER 1:

Key challenges in the development and implementation of data protection laws



Numerous challenges exist to the development and implementation of data protection laws. This study concentrates on seven key areas where action is needed.

A. ADDRESSING GAPS IN COVERAGE

While many global and regional initiatives discussed in this study are designed to enhance interoperability between data protection regimes, a key issue is that enormous gaps still remain in the coverage of data protection laws.

These gaps fall into three broad categories:

1. Countries with no data protection legislation

The number of countries with data protection legislation has grown rapidly in recent years, now reaching a combined total of 108 countries with either comprehensive data protection laws or partial data protection laws.¹⁵ However, this still leaves nearly 30 percent of countries with no laws in place. Personal data receive poor levels of protection in these countries, reducing trust and confidence in a wide range of commercial activities. These countries also risk being cut-off from international trade opportunities, because many trade transactions require cross-border

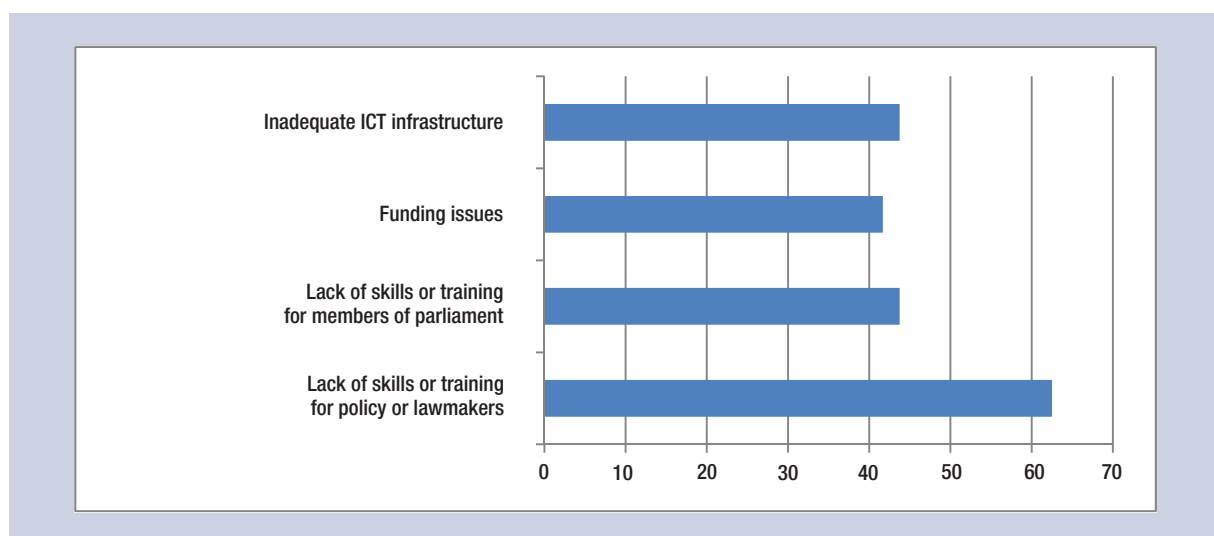
data transfers that are subject to minimum legal requirements. These requirements are difficult (but not always impossible) to meet in the absence of baseline data protection legislation. At least 35 countries are currently drafting data protection laws to address this gap.

However, drafting and implementing data protection laws is a time-consuming and challenging process. Surveys by UNCTAD of government representatives in 48 countries in Africa, Asia and Latin America and the Caribbean point to the need to build awareness and knowledge among lawmakers and the judiciary, in order to formulate informed policies and laws in the area of data protection and to enforce them effectively (Figures 1 and 2). More than 60 percent of the representatives reported difficulties in understanding legal issues related to data protection and privacy.

Similarly, 43 percent of them noted that a lack of understanding among parliamentarians and 47 percent among police or law-enforcement bodies, which can delay the adoption and enforcement of data protection laws, respectively.

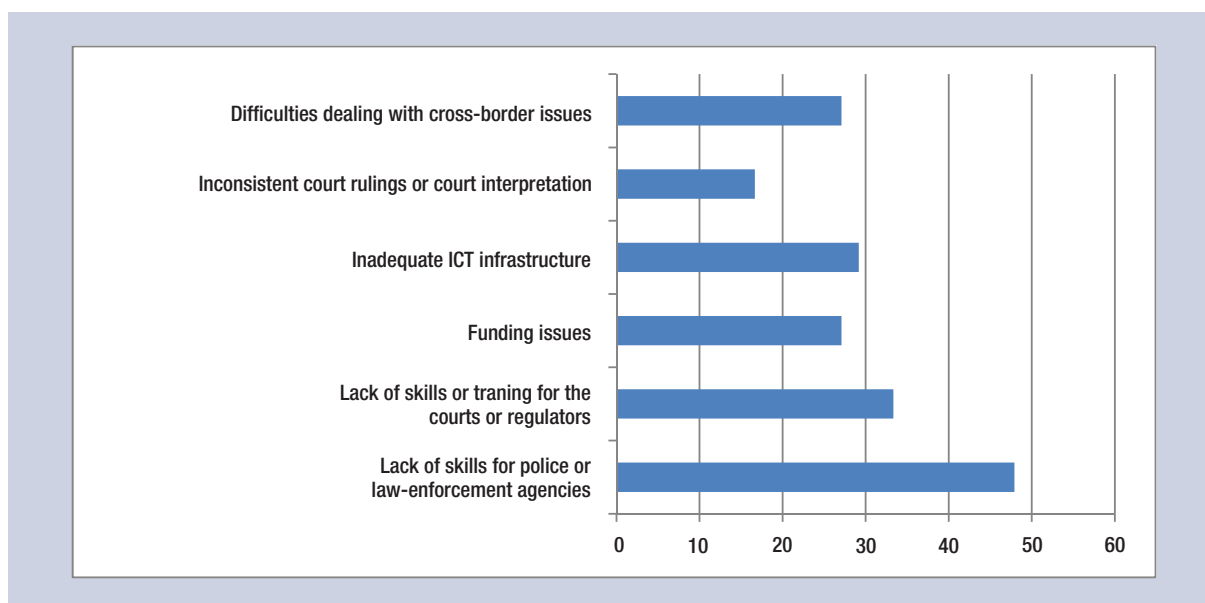
In Part II of this study, several developing countries have provided contributions explaining how the law has been developed in their country. They all report delays and other challenges with resource allocation, capacity and expertise. The experiences of Ghana,

Figure 1. Challenges faced by ASEAN countries and selected countries in the ECOWAS, Latin America and the Caribbean (48 countries) in enacting data protection legislation.



Source: UNCTAD

Figure 2. Challenges faced by ASEAN countries and selected countries in the ECOWAS, Latin America and the Caribbean (48 countries) in enforcing data protection legislation.



Source: UNCTAD

Niger and Uganda presented in Part II are concrete examples of such hurdles faced by those countries.

2. Countries with legislation containing broad gaps and exemptions

Many national data protection laws contain significant gaps and exemptions. For example, some laws exclude small businesses (e.g. Australia and Canada) or small data sets (for example, Japan excludes data sets with less than 5,000 entries) from data protection laws.¹⁶ Other common exemptions apply to: 1) types of data subject (e.g. only to children, or not to employee data); 2) the sensitivity of data (e.g. only to sensitive data like health or financial records); 3) sources of data (e.g. restricted to either online or offline data collection); and/or 4) sectoral data (e.g. exemptions related to the private and public sector, or laws that are restricted to specific sectors like health and credit).

Exemptions are so numerous and complex that an entire textbook could be written just listing and explaining them. They are common in North America and the Asia-Pacific but less common in Europe, South America and Africa, where data protection laws tend to provide comprehensive coverage.

The exemptions create several problems from a trade perspective. They require a wide range of

stakeholders (business, trading partners, consumers and regulators) to identify and categorize data in complex ways. They severely limit opportunities for countries to meet an 'adequacy test' for cross-border transfers (see below). Finally, they can lead to complex complaints and disputes over coverage.

3. Countries where businesses are allowed to exclude certain services or practices from coverage

The third type of gap is less common but has been growing steadily in recent years. Some national laws and regional initiatives allow individual companies to determine the 'scope' of the data protection that they offer to consumers. This can be done in two ways:

First, the company can join a data protection regime (for example, the EU-US Safe Harbor Framework/ Privacy Shield, the APEC Cross-Border Privacy Rules system (CBPRs) or a large range of privacy trustmarks schemes), but limit the scope of their membership to particular activities. The scope is typically published in an online register (see U.S. Department of Commerce list of Safe Harbor members and the APEC CBPRs compliance directory for a variety of scope limitations). Typical limitations restrict coverage to online or offline data collection, consumer or employee data or other broad categories. However, some scope limitations

exclude entire countries from the protection offered by large multinationals (e.g. APEC CBPRs).

Second, the company can exclude certain activities from protection by including fine print exclusions in its public privacy policies. It is increasingly common for organizations to exclude specific services like mobile apps, cloud services and software from the data protection promises that apply more broadly to the business. These exclusions often extend to dispute resolution where the company uses a third party dispute resolution provider, so the exclusions can be quite significant for consumers.

In practice, the second type of exclusion may not stand up to full legal scrutiny if a complaint is made to an appropriate regulator. Regulators have a wide range of powers in this field. For example, key regulators in many jurisdictions can take action against misleading and deceptive conduct. In the United States, the Federal Trade Commission (FTC) can take action for 'unfair' conduct, and this may restrict the use of fine print exclusions. Such specific exclusions are a relatively new development in international data protection regulation, and their status (and future) is uncertain.

Overall, it is challenging to promote global interoperability while these three types of 'gaps' in coverage persist.

B. ADDRESSING NEW TECHNOLOGIES

Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. The relationship between data protection and ICT developments changes all the time, but can be demonstrated by three recent developments.

1. Cloud computing
2. The Internet of Things
3. Big Data analytics

Each of these technologies presents new challenges to data protection, particularly in the areas of the definition of 'personal data' and the management of cross-border data transfers.

1. Cloud computing

The UNCTAD *Information Economy Report 2013*¹⁷ defined cloud computing as a service for enabling

network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration. Cloud services are defined as services that are provided to and used by clients on demand at any time, through any access network, using any connected devices that use cloud computing technologies.

Certain projections estimate that the cloud computing industry will have an estimated global market worth of \$107 to \$127 billion by 2017.¹⁸

Cloud services do not present unique issues in data protection, but they do add to the complexity of existing issues, especially in relation to cross-border data transfers. To date, few jurisdictions have attempted to draft regulations expressly designed to regulate the provision of 'cloud' services. This probably reflects both the broad range of services that fall within the concept of 'cloud', as well as the flexibility of scope within existing regulatory concepts.

Overall, increased interoperability of laws and regimes is important to reduce the likelihood of friction over cross-border data flows for cloud services. In practice, this has been difficult to achieve, and cloud services have in fact become the target of some specific restrictions. For example, Indonesia and the Russian Federation have imposed data localization rules designed to apply specifically to overseas providers of services that are typically delivered via the cloud. As far as is known, Mexico is the only country that has adopted cloud specific provisions in relation to data protection to address transparency about the layered nature of the cloud supply chain; the treatment of user data following service termination, and law enforcement access. The Mexican approach intends to encourage the domestic take-up of cloud solutions. The Republic of Korea also proposed specific laws on cloud computing, although these were broadened following consultation with stakeholders.

The issue of cloud computing and cross-border data transfers is closely linked to the issue of surveillance (discussed in more detail below), since cloud services provided by private sector organizations have become a mechanism for accessing personal data by national security agencies.

Some solutions to this issue are now appearing. For example the United States has recently passed the Judicial Redress Act (JRA) in order to reassure customers of cloud services that they have the same rights to legal redress as U.S. citizens. The Act has a

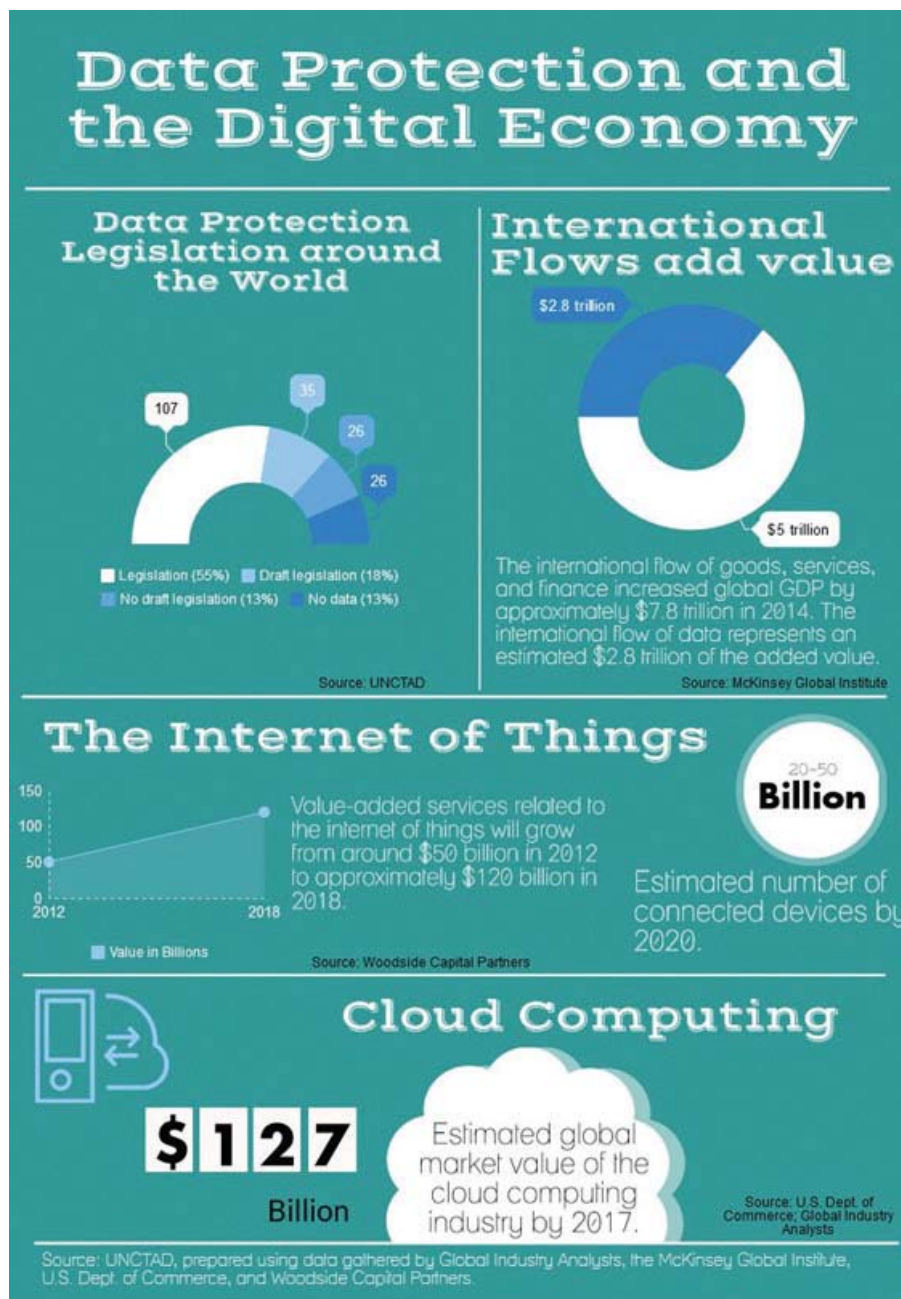
complicated mechanism for assessing who is eligible to exercise these rights, but it is a significant first step in offering dispute resolution options to foreign citizens.

In addition, the cloud service industry has developed and implemented higher standards for privacy and security management,¹⁹ resulting in a 'layered' approach

to protection that may help to increase consumer trust and confidence.²⁰

Overall, cloud services continue to present some challenges for data protection, especially in relation to cross-border data transfers, but there appears to be only a limited appetite for specific laws on the cloud and for restrictive data localization requirements.

Figure 3. Data Protection and the Digital Economy



2. The Internet of Things

The Internet of Things is the term used to describe the numerous objects and devices that are connected to the Internet and that send and receive data. The Internet of Things is also rapidly developing, and has a direct nexus to management of data. A recent BT Intelligence report estimates that the market for Internet-connected devices will be larger than the combined market for PCs, smart phones and tablets by the end of 2016. While forecast reports vary greatly, one study estimates that value-added services related to the Internet of Things will grow from around \$50 billion in 2012 to approximately \$120 billion in 2018, and that there will be between 20-50 billion connected devices by 2020.²¹ Another study forecasts a potential economic impact of between \$3.9 and \$11.1 trillion per year in 2025.²²

A U.S. Federal Trade Commission (FTC) study on the Internet of Things report notes that:

The Internet of Things is already impacting the daily lives of millions of Americans through the adoption of health and fitness monitors, home security devices, connected cars and household appliances, among other applications. Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits.²³

However, the FTC report also notes that connected devices raise numerous privacy and security concerns that could undermine consumer confidence.

Data protection laws have often struggled to keep pace with fast moving developments in technology, but the Internet of Things is probably the largest challenge of this type.

3. Big Data Analytics

Big Data analytics is a methodology for analyzing large data sets to reveal patterns, trends, and associations. It is often cited as the ‘future’ or the ‘solution’ to myriad current problems and issues in society, technology and the economy.

However, the use of Big Data analytics raises a host of privacy issues.

- The sheer scale and value of the data sets involved means that they may be a target for security breaches.

- The data may have initially been collected for a completely different purpose.
- Some data sets are ‘public registers’ and may be exempt from traditional data protection laws (e.g. court records and home ownership records in some jurisdictions).
- The Big Data methodology discourages ‘data minimization’ – the focus is on collecting and keeping all data, since it may be ‘useful’ at some future date.
- Some analysis and decision-making based on Big Data analytics requires the use of rules and algorithms that are not open or transparent to the public.

Big Data analytics is a relatively new approach, and these privacy issues are largely unresolved. There have been some successes in the implementation of Big Data, but there have also been some high profile failures. For example, the U.S. education Big Data portal known as InBloom collapsed despite significant funding and support (over \$100 million was invested in the platform), largely as a result of a ‘privacy backlash’ from concerned parents and educators regarding the potential disclosure to the private sector of data regarding school children.²⁴

Similarly, the initial attempts to leverage National Health Service data in the United Kingdom (the controversial care.data program²⁵) collapsed under the weight of privacy concerns expressed by a range of stakeholders. The project is now proceeding more slowly and cautiously.

Current technologies – cloud services, the Internet of Things and Big Data – as well as future technological innovations and increased connectivity through 5G networks, are all examples of technologies that can deliver enormous benefits, but that carry risks for data subjects. The challenge for data protection regimes is in managing these risks, without restricting or eliminating the potential benefits.

C. MANAGING CROSS-BORDER DATA TRANSFERS

Globally there is a general recognition that there should be some law regarding cross-border data transfers, but a wide variety of approaches to this issue exist, and there is no single global model for managing it.

At the national level, some countries have no restrictions at all on the transfer of personal data to a foreign jurisdiction (the United States is notable for being in this category). Most countries have some sort of restrictions in place, usually accompanied by a long list of exceptions. Typical exceptions fall into two broad categories.

1. One-off exceptions

Over time, a broad consensus appears to have developed in global privacy law regarding the one-off 'exceptional circumstances' that allow a cross-border data transfer to take place. A recent submission by the International Centre for Policy Leadership²⁶ noted that the following exceptions had now become commonplace:

- the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party and (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject;
- the transfer is for the purpose of legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; or
- the transfer is necessary in order to protect the vital interests of the data subject.

This is not an exhaustive list, but it does demonstrate the current 'common ground' in national privacy laws regarding one off exceptions.

2. Ongoing exceptions

The use of ongoing exceptions is less consistent. The following list demonstrates the wide variety of approaches available, but there is no consistency or global consensus in their use.

The 'adequacy' approach (sometimes known as a whitelist approach) assesses whether an entire target jurisdiction provides a sufficient degree of protection for the transfer of personal data. This approach is used by a variety of countries, including the members of the European Union (EU), Israel, Japan and Switzerland.

The 'binding rules' approach considers whether a specific company has put in place processes and independent review mechanisms that provide a sufficient degree of protection for the transfer of personal data (typically within the overall corporate

group). This approach is used in the EU Binding Corporate Rules system (BCRs) and to an extent in the APEC CBPRs. Some individual jurisdictions also have the potential to recognize these types of binding rules, notably Australia and Japan.

The 'model contracts' approach assesses whether the specific wording that appears in contracts provide a sufficient degree of protection for the transfer of personal data. To date this approach has only been used in the EU.

The 'consent' approach examines whether individual consumers are able to consent to the transfer of their data to a foreign country. This approach is available in the EU and some other jurisdictions, but is subject to further conditions regarding the nature of the consent. Consent can be hard to demonstrate and cumbersome for both businesses and consumers, and often gives no guarantee of protection.

Not surprisingly, many countries have chosen to adopt a combination of several approaches to managing cross-border data transfers, since there is no single mechanism that stands out as entirely positive. But the result is that the law regarding cross-border data transfers is fragmented and inconsistent.

A recent development is the emergence of data localization requirements. These require personal data to be retained within their original jurisdiction, either through a direct legal restriction or through other prescriptive requirements (such as local business registration requirements) that have the same result.

Data localization requirements are common in some specific sectors (notably the health sector and the financial services sector), but they are less common for generic data.

There are several drivers for data localization requirements: concern over the potential exposure of local data to increased security risks or surveillance in overseas jurisdictions; concerns about the dominance of foreign countries when it comes to services delivered via the Internet; and government surveillance.

Two often cited examples of data localization requirements are Indonesia and the Russian Federation, which have adopted restrictions on the transfer of data abroad. Businesses face significant compliance burdens in both countries. Other countries considered imposing similar localization requirements (notably Brazil and the Republic of Korea), but after wide stakeholder consultation, they embraced a mixture of alternative approaches discussed above.

Approach	Strengths	Limitations
Adequacy	Enables comprehensive transfer (for those countries found adequate) Promotes interoperability and harmonization Transparent and open 'whitelist'	Causes significant difficulty for those countries that are not found adequate Struggles to accommodate jurisdictions with different approaches to data protection Lengthy process to determine adequacy
Binding rules	Enables free movement of data within a corporate group Promotes best practice data protection processes and oversight in the private sector Transparent and open list of participating companies	Lengthy and expensive approval process Limited use for other data transfers outside the corporate group
Model contracts	Promotes interoperability and harmonization Can be quickly implemented by individual businesses willing to adopt the model contractual clauses verbatim	Challenging to develop appropriate model clauses and to keep them up to date No transparency about who is using model clauses Limited opportunity for oversight
Consent	Quick and easy solution for certain types of transactions No detailed analysis or review required Low compliance burden for businesses	Completely unsuitable for many contemporary transactions Open to differing interpretations of consent and prone to complaints and disputes Potential for lack of fairness in situations where there is a significant power imbalance between the parties Potential to promote fragmentation rather than harmonization of data protection practices

Source: UNCTAD

Data localization requirements are considered to have potentially significant trade implications. They are seen by some observers as going 'too far,' posing risks to trade, innovation and competition. Others also consider that physical localization requirements ignore the reality that logical control over access to data (e.g. encryption keys) is a more important factor for determining the use and abuse of personal data.

The issues arising from cross-border data transfers are to some extent being addressed through international trade agreements (discussed in further detail in chapter 3). One recent example of a relevant agreement is the Trans-Pacific Partnership (TPP) agreement, covering 12 countries. The TPP addresses the issue of balancing data protection against trade considerations. Specifically, it imposes limits on the extent of data protection regulation that signatories can provide in their national laws and builds partly on Article XIV of the WTO General Agreement on trade in Services. Article 14.11 allows restrictions on cross-border transfers if they satisfy four requirements:

- (i) the law must be necessary "to achieve a legitimate public policy objective" – this appears to be very straightforward requirement;
- (ii) the law must not be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination";

- (iii) the law must not be "a disguised restriction on trade"; and

- (iv) the law must "not impose restrictions on transfers of information greater than are required to achieve the objective".

This four-part test appears to be squarely targeting the use of data localization requirements and could set out a potential basis for a global standard for determining whether a restriction has gone 'too far'. The test has good potential to remove 'disguised restrictions on trade', and it may ultimately boost interoperability and harmonization. However, there are a range of views on the likely impact of the TPP.²⁷

Overall, the options for managing cross-border data transfers are many and varied. Some clear consensus has emerged regarding one-off exceptions for specific transfers, but no such consensus is in place for the approval of ongoing transfers. Most countries adopt a mixture of these measures and allow businesses considerable leeway in managing their own cross-border transfers. This is largely driven by recognition of the realities of modern data processing systems, as well as the current volumes of cross-border transfers occurring every moment, which would render any prior-restraint or authorization regime an impossibility.

D. BALANCING SURVEILLANCE AND DATA PROTECTION

It may be difficult to imagine this now, but the relationship between surveillance and data protection was historically treated as something of a ‘fringe’ issue. Many national laws included broad exceptions for law enforcement and national security surveillance.

Global and regional initiatives have also been slow to address the issue of surveillance. Even the European Data Protection Directive does not apply to law enforcement or national security (although this restriction will be removed once the Directive is replaced by the proposed General Data Protection Regulation). Topics like surveillance and national security receive only brief and cursory mentions in the APEC Privacy Framework and the OECD Privacy Guidelines.

The Council of Europe Convention 108 is the only data protection initiative to provide any specific coverage of national security and surveillance issues, and even this coverage is restricted to a minor exemption (Article 9) that allows countries to derogate from just three of the Convention’s provisions (data quality, sensitive data and access rights) in order to protect state security. The derogation is only allowed “to the extent necessary in a democratic society”.

However, the global context for data protection has been changing rapidly; surveillance and national security issues have now come to the fore.

The interest in surveillance began with the growth in cloud computing, which often required personal data to be moved to another country for processing, storage and/or back-up. For example, if the target country was the United States, questions arose about

the potential impact of United States national security legislation (chiefly the PATRIOT Act). Similar issues were raised about other jurisdictions. These concerns were fairly muted and had little impact on the rapid growth of cloud computing until June 2013, when Edward Snowden, a former U.S. intelligence officer, revealed extensive details about the surveillance activities carried out by the intelligence services in the United States and some of their allies.

The new material revealed (or in some cases confirmed) the extent of surveillance of U.S. and non-U.S. citizens. The exact nature and extent of private sector involvement is still subject to debate. The material also revealed that some surveillance activities went beyond the likely expectations of consumers regarding ‘national security’ issues. For example, the material highlighted instances where delegates at a climate change conference were subject to surveillance.

Since June 2013, there has been significant law and policy reform in the U.S. This has included improved governance, restrictions on mass surveillance of U.S. citizens, the extension of some legal rights to foreign citizens, and new restrictions on the operations of U.S. intelligence agencies.

The Snowden revelations also exposed surveillance practices in other countries, notably Germany and the UK, which had previously been unknown to the general public.

Unsurprisingly, numerous legal cases were initiated by consumers and civil liberties organizations to challenge the extent of the surveillance. The cases rely on a mix of constitutional law, treaty law and national laws. There have been several cases in the United States and the UK, but the most significant case is *Schrems v Facebook* (box 1).

Box 1. *Schrems v Facebook* (Ireland, Europe, 2014/2015)²⁸

After the Snowden revelations in June 2013, a well-known privacy advocate (Austrian national Maximilian Schrems) issued a complaint against Facebook in an attempt to prohibit Facebook from transferring his personal data from the EU to the United States. Schrems claimed that the EU-U.S. Safe Harbor Framework did not ensure an adequate level of protection for the personal data of EU citizens, and that the presumption of adequacy that the framework created should be disregarded.

His complaint, which was initially lodged with the Irish Data Protection Commissioner since Facebook’s European headquarters was in Ireland, was dismissed on the basis that Facebook was a member of the EU-U.S. Safe Harbor Framework. That decision was referred to the Irish High Court,²⁹ which referred the matter to the European Court of Justice.

(Continued to page 16)

(Continued from page 15)

The European Court of Justice found that a presumption of adequacy created by Decision 2000/520 (the Decision that approved of the EU-U.S. Safe Harbor Principles as providing an adequate level of protection) did not prevent EU citizens from challenging it on the basis of enforcing their personal rights and freedoms. This finding is of high significance, because it prevents the Safe Harbor or other similar schemes being used as an absolute 'shield' against all consumer claims.

In a dramatic move, the court went further and actually invalidated the EU U.S. Safe Harbor adequacy decision completely. They stated that the Decision was adopted without sufficient limits to the access of personal data and interference by governmental authorities. The court was of the opinion that legislation permitting public authorities to access personal information on a generalized and unspecified basis for reasons related to national security, without providing notice or legal remedy to the individual, was inconsistent with the fundamental rights of EU citizens and did not ensure processing that was "strictly necessary" and "proportionate" as demanded by the EU Data Protection Directive.

The decision is particularly important as it affects trade between the EU and United States corporations, which are among the largest data controllers in the world. As a result, Safe Harbor members no longer enjoy a presumption of adequacy that allowed for the expedient movement of data from the EU to the United States. Going forward, the Schrems court decision seems to set an "essential equivalence" standard for adequacy that has yet to be further defined. This may have an eventual impact on other adequacy decisions and cross-border transfer mechanisms, such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs).

One important result of the case was the renegotiation of the Safe harbor agreement, now to be known as the EU-U.S. Privacy Shield. The new arrangement includes a commitment to stronger enforcement and monitoring, and also includes new limitations and conditions on surveillance.³⁰

Source: UNCTAD, based on various sources.

The task of balancing surveillance and data protection requirements remains challenging. The Schrems v Facebook decision is a direction to place conditions and restrictions on surveillance in any data protection regime in Europe, and this may have knock-on effects on all those jurisdictions that follow European law closely. The United States has initiated multiple reforms that strengthens governance and oversight of the intelligence agencies, and provides consumers with potential avenues for redress.

E. STRENGTHENING ENFORCEMENT

This study is being written at a time when there is a trend towards strengthening enforcement powers and sanctions in the data protection field. This is in response to a series of high profile cases where existing regulatory powers have proved inadequate in

the face of the massive scale and scope of privacy breaches.

Strengthening enforcement powers has been a major theme in amending and updating laws (notably in the Australia, the EU, Hong Kong (China) and Japan).

The United States is considered a leader in this field. Although there are many gaps and inconsistencies in its privacy law, the country has a good record of using massive fines and sanctions to deter privacy malpractice.

The imposition of large sanctions is recognized as being important for: the target company (as a clear signal to senior management and staff regarding reform of their practices); the affected consumers (as an important form of redress for the harm they have suffered); and also as a broader deterrent to the wider industry. The issue of enforcement powers is best demonstrated by some brief case studies (boxes 2, 3 and 4).

Box 2. Office of the Privacy Commissioner for Personal Data v Octopus (Hong Kong, 2010)

The Octopus group of companies provides smart-card payment services and a rewards program in Hong Kong (China). In 2010, as a result of growing public concern (and also revelations by an informant), Octopus was discovered to possibly have been selling personal information of customers to third parties for marketing purposes. It was suspected that Octopus sold information of approximately two million customers, gathered through the applications for its rewards program.

After Octopus finally admitted to transferring the data, the Office of the Privacy Commissioner for Personal Data launched an investigation and produced findings.³¹ The findings confirmed that Octopus' actions violated several data protection principles contained in the Personal Data Ordinance; however, the Commissioner decided that an enforcement notice was not necessary in light of the circumstances and certain corrective commitments made by Octopus.

Many consumers were disappointed that no punishment occurred, and the Ordinance was subsequently amended in 2012 to be less lenient with regards to direct marketing. The amended Ordinance includes stronger consent provisions, a mandatory opt-out opportunity, and a specific procedure that must be followed before personal information is disclosed. Fines for failing to comply were increased to a maximum of \$1 million (HKD).³²

Source: UNCTAD, based on various sources.

Box 3. The Benesse data breach (Japan, 2014)

Benesse is a large Japanese education provider that focuses primarily on correspondence education and publishing. In July 2014, after advertisements had been sent to Benesse customers from a separate IT company, Benesse announced that millions of items of customer information had been leaked as a result of a data breach. The information related to children and their families, and affected tens of millions of customers.³³ It was later found that a systems engineer contracted from an outside firm had breached the Benesse system by copying the information onto his smartphone device, and later selling the information.³⁴

Japan's Personal Information Protection Act (PIPA) is primarily focused on policing the handling of personal information by businesses. After the incident, Benesse issued compensation in the form of cash vouchers to its customers, and committed to handling system maintenance in-house. The incident also prompted the Japanese Ministry of Economy, Trade and Industry to investigate Benesse's security procedures, and to consider amending its guidelines with respect to data security.³⁵

The case, in combination with another large data breach by Japan Airlines, prompted widespread concerns that the previous data protection law was ineffective. In 2015 the Government upgraded and strengthened the legislation; the new law will come into force in 2017.

Source: UNCTAD, based on various sources.

Box 4. FTC v TRUSTe (United States, 2015)³⁶

On March 12, 2015, the FTC issued a complaint against the company True Ultimate Standards Everywhere Inc (TRUSTe) for allegedly violating Section 5 of the Federal Trade Commission Act. TRUSTe is a high profile trustmark and certification company that provides certification marks to clients that meet its program requirements. TRUSTe offers a variety of privacy and security certifications, including an EU Safe Harbor trustmark. Companies can also select TRUSTe as their independent dispute resolution provider.

The complaint (in part) charged TRUSTe with misrepresenting the status of clients' certifications and re-certifications. While TRUSTe's programs claimed to require annual recertification, the FTC alleged that in over 1,000 instances between 2006 and 2013, no annual certification review was conducted. The FTC claimed that this behaviour led to false and/or misleading representations to consumers. The complaint also highlighted several other false and misleading claims made by TRUSTe.

The case was settled, with TRUSTe agreeing to pay a sum of \$200,000, and TRUSTe is now bound by a series of enforceable undertakings regarding its business practices. The case highlights the need for oversight and strong enforcement regarding claims made by intermediaries like TRUSTe.

Source: UNCTAD, based on various sources.

F. DETERMINING JURISDICTION

Determining jurisdiction is a major issue in all important areas of laws, especially cybercrime, taxation and intellectual property law. It has become a very prominent issue in data protection regulation, partly due to the widespread flow of data across borders, partly to the lack of a single global agreement on

data protection (and the consequent fragmentation of regulation).

In the absence of an international agreement, jurisdiction law is complex. It is too large a subject to be covered in this study, but some of the complexity in determining jurisdiction can again be best demonstrated by a few brief case studies (Boxes 5, 6 and 7).

Box 5. US v Microsoft (2014-2015, United States)³⁷

This case deals with the question of whether a warrant, sought under Section 2703 of the Stored Communications Act (SCA) and issued to law enforcement agents of the United States, may be used to obtain information stored on servers outside of the United States. The case is ongoing and is widely considered as a key test of the 'balance' between law enforcement access and individual privacy.

Microsoft owns and operates a variety of web-based services, including e-mail services. Communications are stored in one or multiple of Microsoft's datacenters, some of which are located outside of the United States. In this particular case, law enforcement agents of the United States sought the search and seizure of "information associated with a specified e-mail account" that was "stored at premises owned, maintained, or operated by Microsoft." Microsoft complied with the SCA warrant with regard to information held on servers in the United States, but moved to quash the warrant to the extent that it required the retrieval of information located on a server in Dublin, Ireland.

A federal magistrate judge refused to quash the SCA warrant, on the basis that it applied to information stored outside of the United States. The court asserted that "it has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information."

In examining the elements of extra-territoriality, the court refused to apply the 'presumption against territorial application'. The presumption provides that where statutes are silent on the issue, as was the case here, extra-territorial reach does not exist. Instead, the court pointed to legislative history and practical implications, finding that "an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation."

This case has important implications with regard to governmental requests for information. It sets a precedent that ignores the physical location of data, and focuses instead on the entity in control of the data. The practical implication, as illustrated by this case, is that United States law enforcement agencies may obtain digital information that is located outside of the United States if it is controlled by a U.S. registered company. The case is now the subject of an appeal.

Source: UNCTAD, based on various sources.

Box 6. FTC v Accusearch (2009, United States)³⁸

This case provides an interesting example of cross-border cooperation. Accusearch, Inc. was a company doing business as Abika, operating a website that provided information search services, which could target and profile individuals. Accusearch would forward search requests to third-party researchers, and would then relay the results back to the client as an intermediary.

The case against Accusearch was initiated by the Canadian Internet Policy and Public Interest Clinic (CIPPIC), based at the University of Ottawa. CIPPIC noted that although based in the U.S., Accusearch's actions affected Canadian citizens. CIPPIC first lodged a complaint with the Office of the Privacy Commissioner of Canada (OPC), who initially doubted that its authority extended to policing organizations physically located in the United States. CIPPIC then filed a complaint with the FTC based on violations of U.S. law, and encouraged the OPC to coordinate with the FTC. Both the FTC and OPC ended up pursuing Accusearch through coordinated efforts. The FTC provided the OPC with evidence of Canadian individuals being affected by the company's actions, while the OPC filed an amicus curiae brief supporting the FTC's case in the United States.

(Continued to page 19)

(Continued from page 18)

The complaint noted that some of the searches provided detailed phone records, which are a category of information protected in the United States by the Telecommunications Act 1996. Since telecommunications companies are forbidden from disclosing this information, the acquisition of the information “would most inevitably require someone to violate the Telecommunications Act or to circumvent it by fraud or theft.”

The FTC successfully brought a suit against Accusearch in the United States. The 10th Circuit Court of Appeals confirmed that the FTC has wide latitude to pursue and prevent unfair practices, because the Federal Trade Commission Act generally prohibits “unfair or deceptive acts or practices in or affecting commerce”. An unfair practice can be anything that “(1) causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves, and (3) not outweighed by countervailing benefits to consumers or to competition.”

Source: UNCTAD, based on various sources.

Box 7. Belgian Commission for the Protection of Privacy v Facebook (Belgium, 2015/2016)³⁹

This is the leading case on national jurisdiction in data protection law. At the time of writing of this study, it was the subject of an appeal.

After Facebook changed its privacy policy in 2014, the Belgian Privacy Commission (the Commission) launched an investigation and enlisted Belgian universities to produce a study. The final report, titled “From Social Media Service to Advertising Network: A Critical Analysis of Facebook’s Revised Policies and Terms,” was released on March 31, 2015 by the Katholieke Universiteit Leuven and the Vrije Universiteit Brussels. The report outlined several of Facebook’s practices that were potentially in violation of Belgian data protection law. These included the automatic use of certain “datr” cookies, which were deployed on individuals’ computer hardware when those individuals visited websites on the Facebook domain or certain social media plug-ins that were not on any Facebook domain. The “datr” cookies were employed regardless of whether or not the individual used Facebook services, stayed on the hardware for two years, and allowed Facebook to register the websites visited by the individuals, as well as access other types of information.

In response to the report, the Commission issued Recommendation no. 04/2015 of 13 May 2015, in which the Commission analyzed the legal implications of the technical findings and found that, as relating to non-users of Facebook services, Facebook violated the Belgian Privacy Act and Act on Electronic Communications.

The Recommendation went to the Belgian Court of First Instance, where Facebook argued that it conducted its data processing activities in Ireland through Facebook Ireland Limited and was thus only subject to the data protection authority of that European country. The Belgian Court found that it had authority according to Article 4 of Directive 95/46/EC because Facebook had a subsidiary in Belgium whose lobbying and public administration activities were “inextricably linked” with and thus carried out “in the context of” its data processing activities. In relation to Belgian law, which closely tracks the language of the European Directive, the Court found that by simply storing the data and receiving it automatically Facebook was indeed processing it. Additionally, the Court found that the extent of the processing was not proportional in relation to proffered security advantages, and that it was also processed unfairly due to inadequate consent. Facebook has appealed the decision; however, if Recommendation no. 04/2015 stands, it could signal the end of the “single EU controller” model that many companies operating in Europe have adopted.

Source: UNCTAD, based on various sources.

The question of determining jurisdiction has long been the source of debate and law reform. In the United States, the US Child Online Privacy Protection Act (COPPA) extends to foreign service providers that direct their activities to US children or knowingly collect information from US children. A recent law reform in Japan has resulted in a new requirement (that will come into force in 2017) stating that where a data controller outside of Japan has collected or collects personal information relating to Japanese citizens then

that foreign data controller will be required to comply with key sections of the Japanese Act.

Similarly, the proposed EU General Data Protection Regulation contains an extraterritoriality clause (Article 3) that states:

This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services to such data subjects in the Union; or
- (b) the monitoring of their behaviour.

These reforms are part of a trend towards local data protection regulations attempting to capture any activity that is targeted at local residents, regardless of the actual location of the business.

G. MANAGING THE COMPLIANCE BURDEN FOR BUSINESS

Data protection requirements risk limiting the opportunities for innovation, or creating unrealistic compliance burdens on business (particularly smaller businesses).

Some examples of data protection requirements that have the potential to ‘overburden’ businesses are described below.

1. Registration requirements

In a small number of jurisdictions (mostly in Europe), data controllers are required to register their operations, and sometimes their individual data sets, with the local data protection authority. This requirement has links to the historic establishment of data protection regimes during a period when data processing was seen as the key privacy risk. Over time, some data protection authorities have found the registration process to be a useful form of general regulation and oversight. In many developing countries, the registration process has also become an important income stream for the regulator, which can allow them to work more independently.

Other forms of registration requirements exist in jurisdictions where data protection relies on membership of a specific scheme, such as the EU-US Safe Harbor/Privacy Shield and the APEC CBPRs. Membership in these schemes requires a combination of application payments to the scheme operator (for example, the U.S. Department of Commerce), plus payments to third party providers of dispute resolutions services (like the American Arbitration Association) and/or third party certification services (like TRUSTe). Most fees in these schemes must be paid annually. For businesses the registration requirements can be a burden. Some processes are

time-consuming and bureaucratic, and many of the processes require a one-off or annual payment. The registration requirements also could hamper the ability of businesses to establish one set of data protection processes for use across all jurisdictions.

2. Requirements to appoint data protection officers

A common requirement in national laws is for each business to appoint a specific data protection officer (the name of the role varies slightly in each law). This does not represent a significant burden in most large organizations, where such appointments are common, but it may be a burden on smaller businesses.

3. Requirements to establish data centers or offices in local jurisdictions

In a few rare cases data protection laws require businesses to establish either data centers or an office in a specific location. This issue is discussed elsewhere in the study under the topic of data localization. These requirements present a significant barrier to all businesses, but they are particularly challenging for smaller businesses and new entrants. Overall, they can effectively restrict opportunities for smaller, newer businesses, as well as negatively affect interoperability.

Smaller businesses play an important role in driving innovation and competition, yet they are faced with difficulties operating in jurisdictions with high compliance burdens. There are currently no small businesses registered with either the EU BCR system or the APEC CBPR system.

However, the interests of businesses (including small ones) are not entirely neglected in global/regional and national data protection initiatives. Most of the global and regional initiatives include language warning against complexity, over-burdensome requirements and unintended consequences in the implementation of the regimes. Many initiatives are framed as *enabling* the flow of data as the first priority, subject to appropriate protection as the second priority (e.g. the OECD Privacy Guidelines and the APEC Privacy Framework). Businesses are also extremely well represented in most debates/forums/committees regarding the development, implementation and review of data protection laws.

- ³⁴ Interestingly, the engineer was charged pursuant to Japan's unfair competition act on the basis of stealing trade secrets.
- ³⁵ Bloomberg alert, *Japan Ministry to Amend Data Security Rules as Breached Company Says 48.6M Affected*, September 2015, <http://www.bna.com/japan-ministry-amend-n17179895732/>
- ³⁶ FTC v TRUSTe (United States, 2015), <https://www.ftc.gov/system/files/documents/cases/150318trust-ecmpt.pdf>
- ³⁷ In the Matter of a Warrant to Search a Certain Email Account Controlled by and Maintained by Microsoft Corporation. 15 F. Supp.3d 466 (S.D.N.Y. 2014). See also <http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant>
- ³⁸ F.T.C. v. Accusearch, Inc. 570 F.3d 1187 (10th Cir. 2009), http://www.fasken.com/files/Publication/332cd09f-aae2-4f23-ba5f-3952730ee80f/Presentation/PublicationAttachment/4ffa537e-ca76-4bea-8e93-3a9eef7dc833/cameron_lexis_cplr6_12.pdf
- ³⁹ Willem Debeuckelaere, President of the Belgian Commission for the Protection of Privacy v. Facebook, Inc. Civil Court of First Instance, Recommendation no. 04/2015 of 13 May 2015, 15/57/C (2015), <https://globalfreedomofexpression.columbia.edu/cases/belgian-privacy-commission-v-facebook/>
-

CHAPTER 2: Global developments and lessons learned



Data protection is not the subject of a single, global treaty or agreement. Rather, it is included in a range of international and regional instruments, each of which covers a particular group of countries. These global and regional initiatives differ in their scope and application – many are simply voluntary guidelines.

This chapter discusses the main global initiatives, plus the strengths and limitations of each scheme. Four main initiatives with a near-global reach are discussed in this chapter: United Nations, Council of Europe, the OECD and the IDPC. Each has its own strengths and limitations.

A. THE UNITED NATIONS

The United Nations has a long history of promoting the right to privacy through its Human Rights treaties, particularly through article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. In the period 2013-2015, the United Nations strengthened its role in privacy protection through two high profile measures. The first was the publication of a statement on Digital Rights. The second was the appointment of a Special Rapporteur on the right to privacy.

Statement on the Right to Privacy in the Digital Age

In December 2013, the United Nations General Assembly adopted resolution 68/167, which expressed deep concern for the negative impact that surveillance and interception of communications may have on human rights.⁴⁰ The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.

The Resolution notes that international human rights law provides the universal framework against which any interference to individual privacy rights must be assessed. The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides that no one shall be subjected to arbitrary or unlawful

interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. It further states that “Everyone has the right to the protection of the law against such interference or attacks.”

Other international human rights instruments contain similar provisions. While the right to privacy under international human rights law is not absolute, any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.

The resolution was followed by a detailed report, published in 2014: *The Study of the High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37)*.⁴¹ The report concluded that “practices in many States have ... revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy”.

The Special Rapporteur on the right to privacy

A Special Rapporteur is an independent expert appointed by the UN Human Rights Council to examine and report back on a specific issue.

In July 2015, the Human Rights Council appointed Professor Joseph Cannataci (from Malta) as the first-ever Special Rapporteur on the right to privacy. The appointment is for three years.

The Special Rapporteur is mandated by Human Rights Council Resolution 28/16 to:

- a) gather relevant information, including on international and national frameworks, national practices and experience, to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection, including in connection with the challenges arising from new technologies;
- b) seek, receive and respond to information, while avoiding duplication, from States, the United Nations and its agencies, programmes and funds, regional human rights mechanisms, national human rights institutions, civil society organizations, the private sector, including business enterprises, and any other relevant stakeholders or parties;
- c) identify possible obstacles to the promotion and protection of the right to privacy, identify, exchange

and promote principles and best practices at the national, regional and international levels, and submit proposals and recommendations to the Human Rights Council in that regard, including with a view to particular challenges arising in the digital age;

- d) participate in and contribute to relevant international conferences and events with the aim of promoting a systematic and coherent approach on issues pertaining to the mandate;
- e) raise awareness concerning the importance of promoting and protecting the right to privacy, with a focus on particular challenges arising in the digital age, as well as concerning the importance of providing individuals whose right to privacy has been violated with access to effective remedy, consistent with international human rights obligations;
- f) integrate a gender perspective throughout the work of the mandate;
- g) report on alleged violations of the right to privacy, wherever they may occur, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, including challenges arising from new technologies, and to draw the attention of the Council and the United Nations High Commissioner for Human Rights to situations of particularly serious concern; and
- h) submit an annual report to the Human Rights Council and to the General Assembly.

In March 2016, the Special Rapporteur prepared his first report on the right to privacy, which was submitted to the Human Rights Council (A/HRC/31/64). The report describes his vision for the mandate and provides an insight into the state of privacy at the beginning of 2016 and a work plan for the first three years of the mandate. In order to facilitate the process of further elaboration on the dimensions of the right to privacy and its relationship with other human rights the Special Rapporteur has developed an outline Ten Point Action plan.⁴²

Strengths and limitations of the United Nations initiatives

Strengths of the UN initiatives include:

- wide respect and global coverage;
- a long history of promoting and protecting human rights; and

- a recognition of privacy as a fundamental right.;

Limitations of the UN initiatives include:

- the current treaty provisions are too 'high level' for day-to-day impact – the right to privacy needs to be translated into further detailed principles; and
- the UN faces some significant resource constraints.

B. THE COUNCIL OF EUROPE CONVENTION 108

The Council of Europe Data Protection Convention of 1981 (usually referred to as Convention 108 or the CoE Convention) is the most prominent *binding* international agreement on data protection.

Although this Convention was established by the Council of Europe, its membership is open to any country, and several non-European countries have signed the Convention or are in the process of becoming members.

Forty-six of the forty-seven Council of Europe member States have ratified the Convention and have implemented data protection laws that comply with the Convention (the exception is Turkey where ratification is in progress, the Turkish parliament has recently passed a data protection law⁴³). Uruguay was the first non-European country to become party to the Convention in 2013. Four other countries are currently exploring membership (Mauritius, Morocco, Senegal and Tunisia).

The Convention differs from many other global initiatives in that it is binding on signatories.

Strengths and limitations of the CoE initiative

Strengths of the CoE Convention include:

- it provides comprehensive coverage;
- there is wide acceptance of the principles contained in the Convention;
- it provides the ability for any country to join;
- the Convention works through a collaborative open process;
- the binding nature of the agreement drives harmonization; and
- the Convention has strong support from other initiatives (e.g. it is endorsed by the International

Data Protection Commissioners as the best global model available).

Limitations of the CoE Convention include:

- it has a Eurocentric history (although it is now being rapidly expanded); and
- it faces possible challenges in accommodating very different national schemes (most importantly the U.S.).

Overall, the CoE Convention is the most promising international development in a field where every initiative faces significant challenges.

C. THE OECD

The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* were developed by OECD member states in consultation with a broad group of stakeholders. They were originally published

in 1980 but were revised and re-issued in 2013 (see box 8).⁴⁴ The Guidelines can be followed by any country, not just OECD members.

The OECD itself has 34 members, 32 of which have previously implemented comprehensive data protection laws. In late March 2016, the Turkish parliament passed a data protection bill that is meant to harmonize the Turkish regime with that of the EU, which will leave the United States as the only exception (the U.S. utilizing a sectoral approach to data protection rather than a single law).

However, the real impact of the OECD Guidelines is their influence on the content of privacy laws around the world – well beyond the OECD’s member base. The Guidelines contain eight privacy principles that form the backbone of the principles included in most national privacy laws.

Box 8. Summary of revisions made to the 1980 OECD Privacy Guidelines in 2013⁴⁵

The eight “basic principles” and key definitions remained intact while the rest of the text was updated. The main changes to the Guidelines included the introduction of new text, such as:

- a new section on accountability;
- an updated section on transborder data flows; and
- expanded sections on national implementation and international cooperation.

The revision concentrates on the practical implementation of privacy through an approach grounded in risk assessment and management. Risk assessment helps determine which safeguards are necessary and should be assessed through a process of identifying and evaluating the risks to an individual’s privacy.

Other new concepts to the revised Guidelines include:

- national privacy strategies signalling the increased importance of this policy area along with the need for good cross-department coordination within governments;
- privacy management programmes, which serve as the core operational mechanism through which organizations implement privacy protection;
- data security breach notification, covering both notice to an authority and notice to an affected individual; and
- a new provision calling for ‘complementary measures’ including education and awareness, skills development, and technical tools. It recognizes that privacy laws are necessary but not sufficient.

Subsequent OECD work and milestones

The most recent OECD achievement is the Recommendation on Digital Security Risk Management for Economic and Social Prosperity adopted by the OECD Council in September 2015. It highlights that digital risk should no longer be treated as a technical issue, but as an economic risk. Further, digital risk should therefore be an “integral part of an organization’s overall risk management and decision making.” The OECD Privacy Guidelines and this Recommendation complement each other, and together represent the evolutionary shift towards a more holistic public policy approach to digital risk management. Like the OECD Privacy Guidelines, this Recommendation calls for national strategies and strengthened international cooperation and mutual assistance to tackle increasing digital risk and harness the benefits offered by digital innovation.

Source: OECD

Strengths and limitations of the OECD initiative

Strengths of the OECD Privacy Guidelines include:

- they have a long and respected history;
- the core Principles are widely accepted;
- they have a focus on achieving *balance* between data flows and data protection; and
- they have broad support from a diverse group.

Limitations of the OECD Privacy Guidelines include:

- the absence of a proportionality (or data minimization) principle;
- the non-binding nature of the Guidelines; and
- the developed world focus of the OECD (although in practice the principles are widely influential).

D. INTERNATIONAL DATA PROTECTION COMMISSIONER'S INITIATIVES

The final data protection initiative with a near-global reach is the work of the international Data Protection authorities. Their main role is the regulation of national data protection laws, but because their work involves more international disputes, they have started to involve themselves in the global privacy debate.

Their three main initiatives are: 1) an annual meeting and conference; 2) a system for cooperating in international and cross-border complaints; and 3) a statement on global privacy principles.

This third initiative is of the greatest interest.

At their 2005 meeting, the International Data Protection Commissioners issued a statement titled: The protection of personal data and privacy in a globalized world: a universal right respecting diversities (usually cited as the Montreux Declaration).⁴⁵

The Declaration called for the development of an international convention on data protection, and it is one of the most significant efforts to harmonize data protection laws around the globe.

Specifically, the Declaration stated:

The Data Protection and Privacy Commissioners express their will to strengthen the international recognition of the universal character of these

principles. They agree to collaborate in particular with the governments and international and supra-national organisations for the development of a universal convention for the protection of individuals with regard to the processing of personal data.

To this end, the Commissioners appealed:

- a. to the United Nations to prepare a legal binding instrument that clearly sets out in detail the rights to data protection and privacy as enforceable human rights;
- b. to every Government in the world to promote the adoption of legal instruments of data protection and privacy according to the basic principles of data protection, and also to extend it to their mutual relations; and
- c. to the Council of Europe to invite, in accordance with article 23 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as Convention 108, non-member States of the Council of Europe that already have a data protection legislation to accede to this Convention and its additional Protocol.

Strengths and limitations of the IDPC initiative

Strengths of the International Data Protection Commissioner's initiatives include:

- the significant global influence and profile of the DPCs;
- their real world experience and insight into current issues; and
- the emphasis on the CoE Convention as a global platform (rather than proposing something completely new).

Limitations of the International Data Protection Commissioner's initiatives include:

- a lack of formal structure or follow-up; and
- the non-binding nature of the declaration.

Lessons learned from the global initiatives

These four global initiatives have demonstrated some welcome consistency in the underlying privacy principles - there is a good crossover between the CoE and OECD Principles, with perhaps just some minor concerns regarding the principle of 'proportionality'.

However, only the CoE has had a significant ‘real world’ impact to date. The other initiatives have influenced the development of some laws, but they have not driven effective interoperability. The CoE Convention 108 is the most significant development and sets a benchmark for baseline data protection legislation. The CoE also welcomes engagement with developing nations, and offers the most promise of a global solution.

It is important to note that the U.S. stands slightly aside from these global developments. The U.S. appears unlikely to join any international agreement unless substantial efforts are made to accommodate

their very different approach to privacy protection. However, as we will see in the next chapter, they are more closely engaged with some important regional initiatives.

The following table shows the position of each of the four global initiatives on a ‘spectrum’ for each of the key challenges identified in this study.

Table 2. Strengths and limitations of the main global initiatives in addressing key challenges in the development and implementation of data protection laws

Table 2. Strengths and limitations of the main global initiatives in addressing key challenges in the development and implementation of data protection laws

	Very weak	Weak	Moderate	Strong
Addressing gaps in coverage		IDPC OECD	UN	CoE Convention
Addressing new technologies		IDPC UN CoE Convention	OECD	
Managing cross border data transfer restrictions		OECD	IDPC UN	CoE Convention
Balancing surveillance and data protection	IDPC OECD		CoE Convention	UN
Strengthening enforcement	OECD	UN	IDPC CoE Convention	
Determining jurisdiction	OECD	IDPC UN		CoE Convention
Managing the compliance burden		IDPC UN CoE Convention	OECD	

Source: UNCTAD

NOTES

- ⁴⁰ United Nations, Resolution adopted by the General Assembly on 18 December 2013, 68/167. *The right to privacy in the digital age*, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167
- ⁴¹ United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (an Overview), <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>
- ⁴² See at <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>
- ⁴³ <http://www.dailysabah.com/politics/2016/03/26/turkish-parliament-passes-personal-data-protection-bill>
- ⁴⁴ <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>
- ⁴⁵ The International Data Protection and Privacy Commissioners, *Montreux Declaration - The protection of personal data and privacy in a globalized world: a universal right respecting diversities*, 2005, <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf>
-

CHAPTER 3: Regional initiatives



Regional initiatives are perhaps more developed and mature than global initiatives in the data protection field. Despite some restrictions on membership, regional developments can be influential beyond their immediate boundaries. There is significant divergence in their approaches, posing a potential risk of ‘fragmentation’ that could create barriers to interoperability.

This chapter discusses the main regional initiatives plus the strengths and limitations of each scheme.

Six key regional initiatives are discussed in this chapter, agreements by the European Union, the Asia-Pacific Economic Cooperation, the African Union, the Commonwealth, as well as the Trans-Pacific Partnership Agreement and the Trade in Services Agreement (TiSA).

A. THE EUROPEAN UNION (EU)

The European Economic Area (EEA) has 31 members⁴⁶ and accounts for a significant proportion of the world’s population and global trade. The EU has a long history of involvement in data protection, and this section briefly summarizes several of their key initiatives.

EU Data Protection Directive (1995)

The most significant regional development in data protection regulation is the European Union Data Protection Directive in 1995.⁴⁷ The Directive covers the member states of the European Union, but it has also had a significant influence on global privacy developments.

Its core principles appear in a similar form in numerous national privacy laws outside Europe.⁴⁸

In addition, the cross-border data transfer rules contained in the Directive have set the standard for international data flows for two decades. The Directive includes a mechanism for assessing the ‘adequacy’ of foreign data protection regimes, and this too has proved to be very influential.

Charter on Fundamental Rights

With the coming into force of the Lisbon Treaty in December 2009, data protection became a fundamental right under EU law, related to but distinct from the right to privacy:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

EU General Data Protection Regulation

After more than twenty years of operation, the European Union is ‘upgrading’ the Directive. It is to be replaced by the General Data Protection Regulation (GDPR) – a mandatory regulation that ensures a harmonized approach across all EU member states. The European Commission stated in its contribution:

[T]he GDPR provides for a uniform and simplified legislative framework. It will establish one single pan-European set of rules that will make it simpler and cheaper for companies to do business in the EU, and will ensure that the rights of individuals are more effectively protected across the continent. Consistency of interpretation of the new rules will be guaranteed. In particular, in cross-border cases where several national data protection authorities are involved, a single supervisory decision will be adopted.⁴⁹

The regulation also extends to some sectors that were not previously covered by the Directive, such as law enforcement agencies.

The Regulation is in the final stages of implementation (although a lengthy transition period will apply).

EU Adequacy Decisions

Data protection is a fundamental right for European Union citizens. However, the extent of this protection once any personal data leaves Europe has been a longstanding concern. The EU Data Protection Directive (1995) attempts to address this issue by establishing a series of restrictions (and exceptions) relating to the transfer of personal data outside Europe.

The key provision is Article 25(1), which prohibits EU Member States from allowing the transfer of personal information to countries that do not have adequate protections in place. Importantly, Article 25(6) allows the European Commission to determine that a country has “adequate” privacy protections; EC has approved⁵⁰ the following nations as adequate:

- Andorra, 2010
- Argentina, 2003
- Canada, 2002
- Switzerland, 2004
- Faeroe Islands, 2010
- Israel, 2011
- Isle of Man, 2004
- Jersey, 2008
- New Zealand, 2013
- Uruguay, 2012

In addition, the EC approved the EU-U.S. Safe Harbor Framework in 2000 as a special ‘adequate’ mechanism for U.S. businesses. Under this agreement, certain U.S. companies (not all industry sectors are covered) can voluntarily self-certify that they comply with the Safe Harbor Principles, and thereby be “deemed” adequate under the EU Directive. At the time of writing of this study, the Safe Harbor adequacy decision has been replaced by a draft adequacy decision for the EU-U.S. Privacy Shield.⁵¹

This model for developing a list of “adequate” privacy jurisdictions has been followed elsewhere. For example, Switzerland and Israel both publish lists of jurisdictions where data can be sent because their laws have been approved as adequate, and Japan is in the process of developing a similar list.

EU Binding Corporate Rules (BCRs)

The EU Data Protection Directive (1995) sets out requirements for the transfer of data outside the European Union. These requirements are meant to ensure an adequate level of protection for the data that are transferred, and can be satisfied in several ways. Article 26.2 of the Directive allows for data transfers where an individual data controller “adduces adequate safeguards” through “appropriate contractual clauses.” The Article 29 Working Party thus set out to create a standardized, contract-based set of internal controls and policies so that organizations could easily and independently transfer data within their respective corporate groups. The result became the EU Binding Corporate Rules (BCRs).⁵² BCRs therefore aim to facilitate and streamline compliance with EU data protection law with respect to inter-corporate transfers of data.

The EU BCRs are specific to the countries within the European Union; however, many other privacy frameworks are modeled after or closely track

European Union law. Thus, the use of the EU BCRs system could potentially be expanded. Any company, originating from any country, may subscribe to the EU BCRs system.

Companies or corporate groups must first designate a “lead authority” among the European national data protection authorities if they are interested in subscribing to the EU BCRs program. Next, companies or corporate groups must begin the approval process by drafting their set of BCRs. The European Commission provides a useful toolkit of Working Papers to use and consider during this drafting process.⁵³ There are separate considerations for drafting BCRs for Processors and Controllers. Once the BCRs are approved, the company or corporate group that has adopted them may request authorization to transfer data, based on their approved BCRs, to corporate group entities or branches located outside of the European Union.

The applicant submits their draft BCRs to their lead authority, who must review and comment on the BCRs. After doing so, the lead authority initiates an EU cooperation procedure by providing the draft to other relevant data protection authorities in the European Union (countries from where entities of the applicant intend to transfer data). Some countries in the EU subscribe to a mutual recognition agreement. If the country of the lead authority and another country are part of one of these agreements, then the other country adopts and defers to the lead authority’s evaluations. If that other relevant country is not part of the same mutual agreement, then they must individually consider whether the BCRs comply with the requirements. The cooperation procedure terminates within a month regardless, after which time the BCRs are considered final and the applicant may request authorization.

Currently around 80 companies have subscribed to and complied with the EU BCRs. They are all very large businesses, with about 40 from Europe, 25 from the United States and the rest from other jurisdictions such as Japan.

EU Model Contractual Clauses

The European Commission was vested with the power to draft standard contractual clauses in order to provide guidance to companies and other data controllers in their interactions with customers in the European Union, and to facilitate adequate safeguards that would allow them to transfer data

to other controllers and processors located outside the European Union. The Commission has so far issued three sets of standard contractual clauses; two for transfers between data controllers, and one for transfers to processors located outside the European Union.⁵⁴ By using these clauses in their contracts, controllers are assured that they will be considered, by default, to provide sufficient safeguards pursuant to European Union law.

The Model Contractual Clauses may be used by any data controller to ensure that their policies are consistent with European Union law.

Data controllers may simply use the contract clauses contained in the three currently adopted models in their contracts. The procedure for adoption of the standard clauses, however, is slightly more complicated.

The number of users is almost impossible to gauge, since the system is voluntary and companies may adopt the clauses without being included in a central register. The clauses can also be used for 'one-off' transactions. An estimated several hundred organizations have used the clauses either on an ongoing basis or for one-off transactions.

Strengths and limitations of the EU initiatives

The strengths of the EU initiatives include:

- the EU has strongest set of baseline privacy principles;
- the EU provides comprehensive coverage;
- the EU has mature, well developed data protection case-law;
- the EU Directive has helped to achieve significant consistency within the EU (and this will improve with GDPR);
- the EU has provided the most significant regional leadership in data protection law, with an influence well beyond its boundaries;
- the EU has helped to achieve considerable interoperability through multiple options for cross-border data transfers;
- the EU has grappled with accommodating the different approach to privacy law in the U.S. (not always successfully, but efforts are being made to develop a new EU-U.S. Privacy Shield agreement); and
- the EU has entrenched data protection as a fundamental right and stressed the importance of binding rules.

The limitations of the EU initiatives include:

- the registration requirements (in some but not all member states) are a barrier to many businesses, particularly smaller businesses;
- the EU has sometimes struggled to balance data transfers against data protection;
- enforcement is considered weak and inconsistent by many stakeholders.

B. ASIA-PACIFIC ECONOMIC COOPERATION (APEC)

APEC is composed of 21 member economies that together represent approximately 55 percent of the world's GDP, 44 percent of world trade and 41 percent of the world's population. APEC has developed several recent data protection initiatives.

The three key initiatives are: 1) the development of a set of common APEC Privacy Principles; 2) the development of a system for coordinating complaints that involve more than one APEC jurisdiction; and 3) the development of the Cross-Border Privacy Rules system (CBPRs).

This third initiative is the most relevant for this study, since it has a direct impact on interoperability and cross-border data transfers.

The APEC CBPR system is an innovative self-regulatory mechanism for allowing the transfer of data between APEC members where a company has voluntarily joined the scheme.⁵⁵ The scheme is very new and only a few nations and a handful of businesses are involved, but it represents an alternative approach to traditional measures for managing cross-border data transfers.

The APEC CBPR system provides standard data privacy policies that businesses can use in order to comply with the APEC privacy framework. The system is meant to facilitate cross-border data flows by providing a voluntary framework to ensure certainty and minimum privacy protections.

The APEC CBPRs may be used to demonstrate compliance with the APEC privacy framework, which covers participating APEC economies. There are currently four participating economies: Canada, Japan, Mexico, and the U.S. , although only Japan and the U.S. have approved accreditation agencies in place at this stage.

Businesses may adopt the APEC CBPR principles and policies and then seek accreditation from an approved

third party organization, known as an Accountability Agent.

The Accountability Agent is supposed to certify the organization, and then recertify them each year. Once deemed compliant, organizations are included in a compliance directory.⁵⁶ Organizations are subject to potential enforcement, through law or contract, by Accountability Agents and also privacy enforcement authorities in participating economies.

In theory, other countries will participate in the CBPRs and 'accept' this third party accreditation as a sign of compliance. In practice there are some challenges in implementing such a system.

The APEC CBPRs is a very new program, and as of early 2016, there are only 13 approved organizations, all from the United States.

Strengths and limitations of the APEC CBPRs

The strengths of the APEC CBPRs include:

- APEC has a broad and diverse membership, so there is potential for the scheme to reach a huge market;
- APEC CBPRs is one of the few data protection initiatives that involves the U.S. and has U.S. support; and
- APEC CBPRs provides enormous flexibility in its implementation.

The limitations of the APEC CBPRs include:

- the system is entirely voluntary;
- the system requires business registration and annual fees – these will be a barrier to many organizations; and
- it is unclear what is achieved by membership of the CBPRs in a region where there are numerous complex domestic privacy rules that will always 'trump' the APEC rules.

Overall, APEC CBPRs is a very new, very small scheme. It has some potential, but its overall future impact is uncertain.

C. AFRICAN UNION (AU)

The adoption of the African Union Convention on Cyber-security and Personal Data Protection in June 2014 is potentially very significant. The Convention is unusual in that it aims to establish regional and national legal frameworks for cyber-security, electronic transactions and personal data protection.

The African Union has 54 member states, but the actual impact of the Convention depends on ratifications, and as of early 2016, there are none.

Within Africa, another regional initiative has been developed for the members of the Economic Community of West African States (ECOWAS). The ECOWAS Supplementary Act A/SA.1/01/10 on data protection is unusual as a binding regional agreement. It specifies the required content of data privacy laws and requires member states to establish a data protection authority. To date, seven countries have enacted legislation in compliance with the agreement.⁵⁷

Another regional framework has been developed for the East African Community (EAC) – the EAC Framework for Cyberlaws adopted in 2010.⁵⁸ This framework recommends that each member state develops a regulatory regime for data protection, but makes no specific recommendations on selection of the law.

Strengths and limitations of the AU and other regional African initiatives

The strengths of the AU and other regional African initiatives include:

- the AU is a high profile body with comprehensive membership;
- the AU and other regional African initiatives target developing countries.

The limitations of the AU and other regional African initiatives include:

- the initiatives are very new and do not have significant political support at this stage;
- implementation (especially ratification of the regional agreements) is long and complex; and
- the region experiences considerable resource restraints and challenges in implementation.

Overall, the AU and other regional African initiatives are interesting models/blueprints for developing nations, but their impact is uncertain at this early stage.

D. THE COMMONWEALTH

The Commonwealth is a grouping of 53 nations, supported by a Secretariat. The Commonwealth has contributed to the development of data protection regimes through the influence of Commonwealth

model laws on national legislation of member countries.

The two relevant model laws are the Privacy Bill and the Protection of Personal Information Bill. They both address key issues relating to information privacy. Commonwealth Law Ministers recommended the model Bills to member countries for adoption (or adaptation to national circumstances) as Commonwealth models of good practice.

The adoption of the model laws by several countries has had a positive impact on harmonization. The principles contained in the model laws are heavily influenced by the OECD privacy guidelines and the EU Directive, although there is considerable flexibility in their implementation. The Commonwealth also provides some technical assistance and capacity-building assistance to its members, particularly less developed member countries in Africa, the Caribbean and the Pacific.

Strengths and limitations of the Commonwealth initiative

- The strengths of the Commonwealth initiative include:
- the Commonwealth has a large and diverse membership;
- some technical assistance and capacity-building assistance is available; and
- the Commonwealth is able to target some regions (such as the Caribbean and the Pacific) where there are limited opportunities for the development of data protection regulations.

The limitations of the Commonwealth initiative include:

- the initiative is non-binding;
- the Model Privacy Bill does not address many key issues, such as cross-border data transfers; and
- it only extends to data held by “public authorities”, not private sector.

Overall, the Commonwealth initiative is fairly limited, but it does help to reach some nations that are not part of other regional initiatives.

E. TRADE AGREEMENTS

Trade agreements have emerged as a new source of both data protection law and guidance on managing the potential conflict between data protection law and cross-border data flows. There is a range in

the types of agreements – from simple bilateral free trade agreements to complex regional and global agreements.

One difficulty in examining these agreements is that during the negotiation phase the documents are not available for public review.

However, one example of a relevant agreement that has now been made public is the Trans-Pacific Partnership Agreement (TPP).

Twelve countries - Australia; Brunei Darussalam; Canada; Chile; Japan; Malaysia; Mexico; New Zealand; Peru; Singapore; the United States; and Viet Nam – have joined the Trans-Pacific Partnership Agreement (TPP). The agreement was signed in October 2015. Its primary aim is to establish a new free trade area; it will be a binding agreement once all 12 countries have ratified it.

The TPP is unlike most of the other data protection instruments discussed in this study, in that it does not really impose any significant positive requirements for data protection, but it does address the issue of balancing data protection laws against trade considerations. Specifically, it imposes limits on the extent of data protection regulation that signatories can provide in their national laws.

Article 14.8 requires parties to “adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce”. A note to the Article states that “for greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy”. There are no further requirements and the impact of this requirement is likely to be very limited.

Article 14.11 concerns ‘Cross-Border Transfer of Information by Electronic Means’. It requires that cross-border transfers of personal information be allowed when the transfer relates to the business practices of an organization in a TPP member country.

Importantly, this article only allows restrictions on cross-border transfers if they satisfy four requirements:

- (i) the law must be necessary “to achieve a legitimate public policy objective” – this appears to be very straightforward requirement;

- (ii) the law must not be “applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination” – this requirement basically states that the restriction must apply to everyone, meaning that foreign companies will be subject to the same legal restrictions as domestic companies;
- (iii) the law must not be “a disguised restriction on trade” – this is new wording and is the most interesting rule in the TPP. The result is that any business affected by a cross-border transfer restriction can challenge the law as a “disguised restriction on trade”. This would be a difficult task for anything other than the most extreme restriction. This clause appears to establish a new balance between privacy protection and trade restrictions, and in the future this wording may become a common part of international agreements.
- (iv) the law must “not impose restrictions on transfers of information greater than are required to achieve the objective”. This clause could be very subjective in practice, and may provide some room for disputes.

If a restriction on cross-border transfers goes too far, and breaches one of these four tests, it could be challenged under the TPP dispute resolution procedures.

As stated earlier, the TPP establishes a new approach to balancing privacy protection and trade. The four-part test may prove successful, and it would not be a surprise if the same (or similar) wording appeared in other international trade agreements.

Other significant agreements that are under consideration include the TiSA and the TTIP.

The Trade in Services Agreement (TiSA) is a potential trade agreement between 50 parties, including the European Union (and therefore its members), Japan, the United States and a very diverse range of other countries. The agreement aims to remove tariffs and other trade barriers in the global trade of services such as banking, health care and transport.

The text of the agreement is secret, but it appears that at least some provisions on data protection will be included in the agreement. The involvement of the EU in TiSA means that it is unlikely that national data protection requirements will be significantly weakened, but wording similar to the TPP may appear in the final

text, setting out a ‘test’ for balancing data protection requirements against the cross-border flow of data.

The Transatlantic Trade and Investment Partnership (TTIP) is a potential free trade agreement between the European Union and the United States. It covers goods, services, investments and industry sector regulation. The text is secret and it is unclear whether data protection will be included.

The strengths and limitations of international trade agreements:

The strengths of international trade agreements include:

- they have the potential to engage with a very wide range of countries – in theory there are no regional limitations, although regional agreements are now more common than global agreements;
- they are binding on the parties and they have the potential to drive interoperability; and
- they have the potential to address the balance between data flows and data protection.

The limitations of international trade agreements include:

- negotiations are complex and secretive;
- consumer and civil society stakeholders are often excluded from the development of trade agreements;
- they contain complex dispute resolution procedures and there is a history of significant disputes and conflicts.

Overall, trade agreements have enormous potential for influence on national laws. However, they also have enormous potential for conflict or legal challenges, and there is a long history of international disputes relating to trade agreements. In the future, it is possible that data protection law will be influenced by disputes brought under these agreements – so the content of the agreements is vital.

Lessons learned from the regional initiatives

The regional initiatives have been the key driver for data protection regulation (particularly the EU initiatives). Some potential exists for fragmentation and divergence with the large number of competing initiatives, and their lack of comprehensive coverage. Some interesting crossovers are developing (for

example the ongoing cooperation between the EU and APEC concerning binding corporate rules); this type of collaboration needs to be developed further.

Some regional initiatives (OECD, The Commonwealth) are still based on voluntary principles and model laws, and their relevance today is diminishing. The current priority is on implementing and enforcing (and where possible harmonizing) actual regulations, although principles and model laws have provided some very useful guidance in the past.

The emergence of trade agreements as a key factor in data protection regulation is a new development, which

has the potential to highlight the trade implications of data protection.

The following table shows the position of each of the seven regional frameworks on a 'spectrum' for each of the key themes of this study (note that the EU is split between the EU Directive and the EU GDPR).

Table 3. Strengths and limitations of the main regional frameworks in addressing key challenges in the development and implementation of data protection laws.

Table 3. Strengths and limitations of the main regional frameworks in addressing key challenges in the development and implementation of data protection laws

	Very weak	Weak	Moderate	Strong
Addressing gaps in coverage	Trade Agreements	OECD APEC Commonwealth	EU Directive ECOWAS	EU GDPR AU
Addressing new technologies		APEC Commonwealth AU ECOWAS	OECD Trade Agreements EU Directive EU GDPR	
Managing cross border data transfer restrictions		OECD Commonwealth	EU DIRECTIVE Trade Agreements APEC AU ECOWAS	EU GDPR
Balancing surveillance and data protection	APEC Commonwealth	OECD AU ACOWAS		Trade Agreements EU Directive EU GDPR
Strengthening enforcement	APEC OECD Commonwealth Trade Agreements	AU ECOWAS	EU DIRECTIVE	EU GDPR
Determining jurisdiction	OECD APEC Commonwealth	Trade Agreements ECOWAS	EU DIRECTIVE AU	EU GDPR
Managing the compliance burden	Commonwealth	APEC EU Directive EU GDPR	OECD AU ECOWAS	Trade Agreements

Source: UNCTAD

NOTES

- ⁴⁶ The European Economic Area comprises the 28 European Member States plus Iceland, Liechtenstein and Norway.
- ⁴⁷ 1995 *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (95/46/EC)
- ⁴⁸ More specific information on the principles governing, and rights afforded by, the Directive can be found in the contribution by the European Commission in Part II.
- ⁴⁹ See the contribution by the European Commission in Part II. The contribution contains further details concerning the updates included in the GDPR.
- ⁵⁰ http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- ⁵¹ The draft adequacy decision and supporting documents are available here: http://europa.eu/rapid/press-release_IP-16-433_en.htm?locale=en
- ⁵² http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm
- ⁵³ The Working Papers may be found here: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm
- ⁵⁴ http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm
- ⁵⁵ More information on the APEC CBPR system can be found here: <http://www.cbprs.org/default.aspx>
- ⁵⁶ The Directory is available at www.cbprs.org
- ⁵⁷ See http://unctad.org/en/PublicationsLibrary/dtlstict2015d2_en.pdf
- ⁵⁸ See http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf
-

CHAPTER 4: Select national initiatives and experiences



According to UNCTAD's Cyberlaw Tracker, as of April 2016, 108 countries have implemented national data protection laws. The laws are all slightly different, but they share the objective of regulating the collection, use and disclosure of personal information. Ninety-five of the laws are specific comprehensive data protection laws. Twelve of the laws provide data protection through a sectoral approach or are sub-sets of other e-commerce or consumer protection legislation. The impact of the law in these jurisdictions may depend on the type of business or the type of transaction. In addition, an additional 35 nations have draft data protection legislation. These draft laws are a mix of comprehensive and sectoral data protection laws.

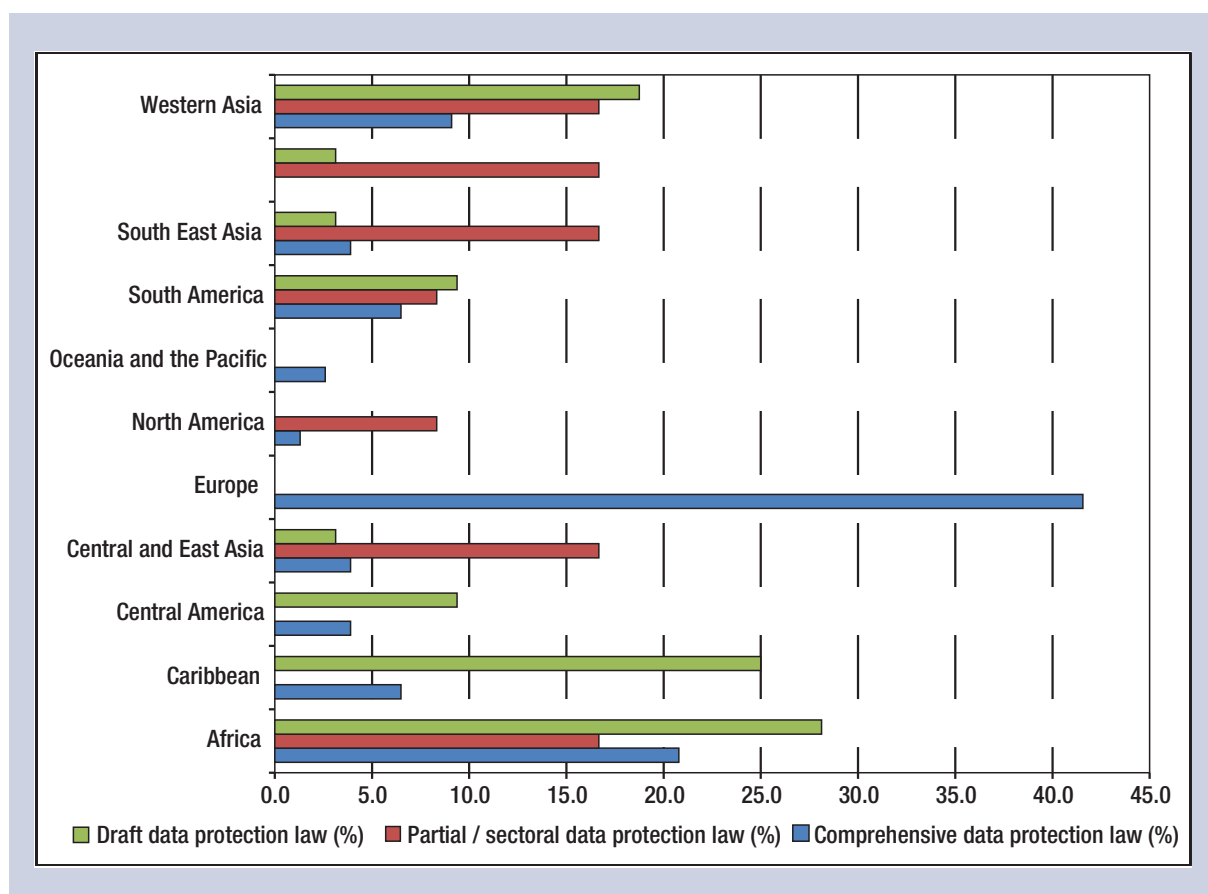
Approximately 60 developing countries still do not have data protection laws in place.⁵⁹

Traditionally, data protection law has been dominated by European jurisdictions, but in recent years data protection has spread across the globe to become a truly international phenomenon.

Figure 4 shows the number of data protection laws in each region according to three categories: comprehensive, partial/sectoral and existing draft laws.

The "comprehensive" category includes countries with a specific data protection law that generally covers the entire private sector in all their activities, although there may be a few small gaps and exceptions. The "partial/sectoral" category includes countries with either single or multiple laws that collectively provide data protection for some sectors or activities.

Figure 4. Global percentage of comprehensive, partial/sectoral and draft data protection laws in each region



Source: UNCTAD

Country snapshots

The following sections provide a snapshot of data protection legislation in select jurisdictions. The countries have been chosen in order to display the diversity of legal approaches that have been taken. Some of the examples concern data protection laws in developed countries, but they still provide useful lessons for developing countries.

Australia

Australia is a good example of a country that has amended and expanded its privacy legislation over many years, resulting in an up-to-date law with fairly comprehensive coverage. The law still exempts some small businesses and completely excludes employee records, but is otherwise closely aligned with international data protection models.

The Privacy Act 1988 (Cth) requires private-sector organizations to comply with the Australian Privacy Principles in their collection, use, disclosure and handling of an individual's personal information. The legislation was significantly amended in 2012, resulting in increased penalties and a wider range of powers for the regulator (These amendments came into effect in 2014).

In addition, some Australian states and territories have their own privacy legislation covering state government agencies and/or health providers.

The Australian law is broadly compatible with the EU Directive (apart from the exemptions for small business and employee records), but Australia has never been granted 'adequacy' status by the EU. Australia is also a member of APEC and the current privacy legislation is compliant with the APEC Privacy Framework. However, Australia is not a participant in the APEC Cross-Border Privacy Rules scheme (APEC CBPRs) at this stage.

The key regulator is the Privacy Commissioner at the Commonwealth level.⁶⁰ Similar bodies are in place in some states.

One interesting aspect of the Australian regime is that there are no registration requirements for private-sector organizations in Australian privacy law. The international transfer of personal data is restricted unless organizations can meet certain requirements. These include consent, storage standards and the legal protection of the data in the recipient country.

Brazil

No general privacy or data protection law currently exists in Brazil, but it is a good example of a country that has been attempting to develop draft data protection legislation. A Draft Bill for the Protection of Personal Data was released in January 2015. It is broadly based on the European Data Protection Directive.

In the meantime, privacy is a guaranteed right under Article 5 of the 1988 Constitution. The Constitution also provides for the innovative right of 'habeas data', which gives consumers the right to know what data are held about them and to correct it. In addition, some limited additional statutory protection for privacy can be found in the Consumer Protection Law 1990. Also, the Brazilian Internet Civil Rights Law, Federal Law No. 12965/2014, provides numerous legal rights for Brazilian citizens and Internet users, including protection about collecting and sharing personal data; its scope is limited to on-line activity.

There are no cross-border data transfer restrictions in Brazil – and it is unclear what exact form these might take in the draft Bill. The 2015 Draft Bill requires explicit consent to transfer personal data with limited exceptions and restricts the transfer of personal data only to countries that provide an equivalent level of data protection to Brazil.

Finally, Article 11 of the Internet Civil Rights Law, Federal Law No. 12965/2014, prescribes that, if any act that includes collection, storage, custody and treatment of data by a service provider occurs within the national territory of Brazil, it must respect Brazilian law and rights. This does not, however, place any specific restrictions on the transfer of data.

As stated in by the Brazilian Institute of Consumer in Part II of this study:

"International data flows are allowed as long as they comply with Law 12.965/14. However, Brazil needs more norms and institutional structures. In a world of increased complexity and with the rise of specialized global policy communities, Brazil is missing an opportunity to create one agency dedicated to this issue and collaborate in a global level for better regulations, compliance and protection of collective rights."

Brazil did consider some data localization requirements in response to the Snowden revelations in 2013 and 2014, but eventually decided against them.

France

France is a good example of an established data protection regime under the EU Directive. It is also an interesting example of the use of complex 'registration requirements'.

The Data Processing Act 1978 (revised 2004) sets out the main data protection provisions in France. Several other laws contain minor data protection requirements.

The National Commission on Computer Science and Freedoms (Commission nationale de l'informatique et des libertés) (CNIL)⁶¹ is an independent administrative authority protecting privacy and personal data. CNIL is probably one of the most visible and active privacy regulators in the world.

Like many European data protection laws, some registration requirements are in place. Chapter IV of the Data Processing Act sets out the required formalities for data processing. Depending on the type of data processing involved, the data controller must comply with one of four different sets of formalities, ranging from simple notification to authorization. These rules are complex. Authorization is generally restricted to activities that are "deemed potentially harmful to privacy and liberties".

Article 23 of the Data Processing Act 1978 sets out complex rules for the notification and authorization of cross-border transfers:

- transfers within the EU do not require notification or authorization;
- transfers to countries formally declared as 'adequate' by the EU requires notification only; and
- transfers to all other countries require authorization.

India

India is an example of a country with a complex, sectoral approach to data protection. India does not have a stand-alone data protection law; those protections that are available are contained in a mix of statutes, rules and guidelines.

The most prominent provisions are contained in the Information Technology Act, 2000, as amended by the Information Technology Amendment Act, 2008. In particular, Section 43A, which addresses 'reasonable security practices and procedures' is complemented by the Information Technology (Reasonable Security

Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

However, the scope and coverage of these rules is limited:

- the majority of the provisions only apply to 'sensitive personal information';
- the provisions are restricted to corporate entities undertaking the automated processing of data; and
- consumers are only able to take enforcement action in relation to a small subset of the provisions.

In order to address these limitations, India has been considering implementation of a comprehensive privacy law for some time. The draft Right to Privacy Law 2014 law is being considered by the Government, but its exact progress is uncertain.

At this time, India does not have a central, national regulator or complaints body for data protection. The draft Right to Privacy Law being considered would establish a national Data Protection Authority of India (DPA).

Some very limited rules are in place for the transfer of sensitive data offshore. Data can be transferred only to a country where it is clear that the sensitive data will be adequately protected (Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011). "Sensitive data" is defined under the 2011 rules as information relating to a data subject's password, financial information, health, sexual orientation, medical records, and biometric information.

Indonesia

Indonesia is a good example of a jurisdiction that has introduced a data localization requirement.

The Law on Information and Electronic Transactions of 2008 contains a very brief section on privacy (Article 26). A regulation under the Act (Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions) provides more detail. Electronic system providers must ensure the protection of any personal data that they process. Such protection broadly includes obtaining necessary consent and ensuring that personal data are used only in accordance with the purpose communicated to data subjects. The Indonesian approach is not based on any international model.

Indonesia has yet to establish a data protection regulator. While the legislation is silent on the establishment of a regulator, this may be covered in future regulations.

Indonesia is one of the few developing countries to have introduced general data localization requirements related to data processed for public services. Article 1 of the Draft Ministerial Regulation concerning Data Center Technical Guidelines states that

“Any Electronic System Administrator for public service shall place a data center and a disaster recovery centre in Indonesia.”

Also, Article 17 (2) of the Regulation on Electronic System and Transaction Operation states that

“Electronic System Operation for public services shall place a Data Center and disaster recovery center in the territory of Indonesia for law enforcement, protection and sovereignty of the state and its citizens.”

These provisions are very recent, and their impact has not yet been measured.

Japan

Japan is a good example of a country that has recently amended its privacy laws to address specific problems with enforcement.

The Act on Protection of Personal Information (APPI) 2003 has applied to the private sector since 2005. The law covers both the public and private sectors.

A substantial amendment to the APPI was passed on 3 September 2015. (This will not come into full effect until 2017.) The current law (still in force today) contains a general exemption for organizations that hold fewer than 5,000 records. However, this exemption has been removed in the recent amendments.

Although Japanese law contains some unique provisions, the core principles are based on a mix of the OECD Guidelines and the EU Directive. Japan is also a member of APEC, and the Japanese privacy law complies with the APEC Privacy Framework. Japan is a formal participant in the APEC Cross-Border Privacy Rules system (CBPRs).

The 2015 amendments to the law are expected to be supported by implementation guidelines developed by the new Personal Information Protection Commission (PIPC). An early draft of the implementation guidelines includes a proposed provision recognizing the APEC

Cross-Border Privacy Rules scheme (APEC CBPRs) as binding for the purposes of cross-border data transfers. Once in force, this provision could act as an exemption to cross-border rules in the Japanese legislation, where the receiving company is a certified APEC CBPRs participant.

The original Act on Protection of Personal Information (APPI) 2003 did not establish a central privacy regulator in Japan. Instead, each sectoral regulator took on the role of privacy regulator for that sector. This was seen as a major deficiency of the existing regime. The amendments to the APPI establish a new Personal Information Protection Commission (PIPC). The PIPC will have significant powers, including audit and inspection powers, and the power to request that companies submit compliance reports. The amendments also allow companies to buy and sell personal data that has been anonymized or aggregated – this provision has been included to enable (and encourage) the use of big data analytics in Japan.

A range of EU-style rules apply to data transfers for both domestic and global third party service providers, including a requirement to supervise subcontractors when data are transferred to a third party. The 2015 amendments to the Act on Protection of Personal Information (APPI) set out a more comprehensive set of rules for cross-border transfers, but also include certain exceptions.

The new amendments in Japan are considered to be a significant improvement.

Republic of Korea

South Korea's privacy law is contained in the Personal Information Protection Act (PIPA) 2011, a comprehensive data protection law. PIPA was amended in 2013, 2014 and 2015.

The key privacy principles are based on a mix of the EU Directive and the OECD guidelines, with some variations.

Korea is also a member of APEC, although Korea does not participate in the APEC Cross-Border Privacy Rules scheme (CBPRs) at this stage.

Korea has a unique dispute resolution system for privacy. In the event that a user suffers damage from an organization violating the information protection provisions, the user may claim compensation from the provider. In this case, the provider will be held

responsible if it fails to prove the non-existence of an intention to infringe, or the absence of negligence causing such violations. Claims for damages may be filed with the Personal Information Dispute Mediation Committee.

Russia

Russian privacy law is complicated. The key legislation is Federal Law No. 15-FZ on Personal Data 2006 (the Personal Data Law), which is supplemented by numerous additional laws, regulations and guidelines, including:

- provisions on methods and means for protection of personal data information systems, enacted through Order by the Federal Service for Technical and Export Control No. 58 dated 5 February 2010;
- government Resolution No. 781 dated 17 November 2007, on establishing the regulations for providing security of personal data while processing personal data information systems; and
- main procedures for organizing and technical support for the security of personal data processed in personal data information systems enacted on 15 February 2008.”

The combination of a number of Russian laws provides comprehensive privacy protection across all sectors.

The Russian law has many similarities with the EU Directive. However, enforcement of the law appears to be limited. Russia is a member of APEC but does not participate in the APEC Cross-Border Privacy Rules system (CBPRs).

An interesting aspect of Russian law is that Article 110 of Federal Law no. 149-FZ on Information, Information Technologies and Protection of Information provides citizens with a ‘right to be forgotten’ and can be used to remove some URLs from search results.

The key regulator is the Federal Service for Super-vision in the Sphere of Telecommunications, Informational Technologies and Mass Communications (Roskomnadzor)⁶².

In Russia, the collection and processing of data requires formal registration by the data operators with the Roskomnadzor. There are exceptions for simple, one-off collection of data and human resources data.

Overseas transfers are subject to the same registration requirements as domestic collection and processing.

From September 2015, however, it is a legal requirement that data operators store the personal data of Russian citizens on servers based in Russia. The Roskomnadzor is tasked with implementing this law. Large foreign-based data operators have been given extra time to comply with the law (until early 2016). The law only applies to data collected or updated after September 2015.

South Africa

South Africa’s comprehensive privacy law, the Protection of Personal Information Act 2013, was enacted in August 2013. The legislation covers all sectors. It is one of the most recent examples of a new privacy law in a significant market.

The Act was based on, and is compatible with, the EU Data Protection Directive. The Information Regulator is the national privacy regulator of South Africa, an independent body with a national jurisdiction.

There are no registration or notification requirements in South Africa.

Cross-border transfers are forbidden unless they satisfy certain requirements - most notably that the recipient is subject to a law, code or contract that ensures a level of privacy protection equivalent to that of South Africa.

United Kingdom

The Data Protection Act 1998 (DPA) is a comprehensive privacy law for the public and private sectors. It has been updated several times. The legislation is comprehensive and covers all sectors. The Data Protection Act 1998 implements the EU Data Protection Directive.

Article 8 of the Human Rights Act 1998 is also important in the UK. It provides a right to respect for private and family life, home and correspondence. The provision is sometimes used in actions related to privacy breaches by the media.

The Information Commissioner’s Office (ICO)⁶³ is the UK’s independent data protection regulator.

Data controllers must register with the Information Commissioner’s Office to report their intention to process personal data before they begin. Fees and an annual renewal requirement apply. There are a small number of exemptions to the registration requirement.

The Data Protection Act allows data to be transferred to non-EU countries, subject to a range of conditions (such as consent and contract).

Lessons learned from national data protection laws

A large number of national data protection laws are in place, and although each law is slightly different, some interesting lessons can be learned from the overall trends in their development.

For example, lessons can be learned from the most *recent* countries to introduce data protection legislation (such as Malaysia, Singapore and South Africa).

It is notable that in each of these jurisdictions, the laws included:

- high level principles, with less detailed prescription;
- the establishment of a single independent national data protection regulator;
- the complete absence of ‘registration’ requirements;
- high-level (non-prescriptive) provisions enabling cross-border data transfers, subject to some conditions; and

- lengthy transition periods for local business compliance.

Lessons can also be learned from the most recent countries to amend data protection legislation (such as Australia, Canada, Japan, New Zealand, Poland and Russia). There is less consistency amongst this group, but some key lessons have emerged.

Some of the key drivers for amending privacy legislation in these countries included:

- a perceived need to strengthen the powers of data protection regulators, particularly in relation to increased sanctions;
- the removal of exemptions and exclusions;
- a desire to simplify (and centralize) data protection regulation in a single national agency; and
- the expansion of data protection requirements to include matters related to security, particularly data breach notification requirements.

NOTES

⁵⁹ See “Digital Globalization: The New Era of Global Flows.” McKinsey Global Institute, March 2016. <http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>. <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

⁶⁰ www.oaic.gov.au

⁶¹ www.cnil.fr

⁶² www.rkn.gov.ru/eng/

⁶³ www.ico.gov.uk

CHAPTER 5: Private sector and civil society perspectives



Two key stakeholders in the discussion of data protection and international data flows are the private sector and civil society. This chapter briefly discusses their perspectives.

A. THE PRIVATE SECTOR

The private sector makes regular contributions to the debate on data protection and international data flows.

Some of their key recent interventions include:

- publication of data on the importance of maintaining international data flows, particularly in defence of the EU-U.S. Safe Harbor Framework;⁶⁴
- joint letters and campaigns to the U.S. Government on the need to improve controls and oversight relating to national security surveillance, following the Edward Snowden revelations in June 2013;⁶⁵
- joint letters and campaigns to several national governments supporting the need for strong encryption to be available for commercial use, without providing ‘backdoor’ access to Government and law enforcement agencies;⁶⁶
- submissions to national reviews of data protection laws, in particular submissions to Japan urging them to appoint a national data protection regulator rather than persisting with over 30 separate regulators;
- research and campaign material on the negative impact of data localization requirements; and
- numerous submissions to national law reform processes on the need to manage cross border data transfers in a consistent and balanced way (for example Australia, Indonesia and Japan).

The private sector has also been instrumental in driving some specific data protection mechanisms. The APEC CBPRs is a good example of a data protection regime that has been initiated and promoted by both Government and business. It is an example of a recent trend for the private sector to be directly engaged with policy development regarding privacy, rather than being a passive observer or simply ‘responding’ to Government policy initiatives.

Through all of these initiatives, the private sector has presented a fairly clear and consistent set of arguments on the need to balance data protection

and data flows. Their overall position usually includes the following arguments:

- governments should only intervene in the market to the minimum degree necessary to ensure that trade is fair and that fundamental rights are protected;
- data protection laws should be based on broad principles rather than highly detailed or prescriptive requirements;
- there should be no specific laws for specific technologies (e.g. cloud, big data, the Internet of Things) – the private sector prefers generic legal principles that can apply to a wide range of technologies;
- the private sector should not be treated as an agent for law enforcement or surveillance – requests for assistance should be minimal and subject to strong oversight and conditions;
- the private sector should be free to disclose the nature and extent of government and law enforcement requests for access to data;
- data protection laws, and more specifically cross-border data transfer rules, should not create significant compliance burdens, especially for smaller businesses; and
- cross-border data transfer rules should allow organizations some flexibility in how they comply (usually by providing a variety of approved mechanisms).

Interestingly these private sector policy positions are supported by a wide range of stakeholders both inside and outside the private sector.

The private sector has also expressed some support for strong enforcement, particularly the use of fines and sanctions by the Federal Trade Commission in the United States.

There are numerous examples of this support, but the most often quoted statement comes from the *Essentially Equivalent report - A comparison of the legal orders for privacy and data protection in the European Union and United States* (Sidley 2016):

Coordinated and comprehensive privacy regulation combined with active enforcement and sizable fines establish a strong deterrent to motivate compliance with US privacy and security requirements - perhaps even stronger than in the EU.⁶⁷

Overall, the private sector has played an important role in ensuring that the right balance is struck between data protection, innovation and competition. They have also drawn attention to the difficulties faced by smaller businesses in complying with some specific data protection requirements.

B. CIVIL SOCIETY

The civil society/consumer perspective is also quite prominent in the data protection debate, although civil society representatives have fewer formal opportunities to engage in important policy developments. For example, civil society is often excluded from the drafting and negotiation process in the development of regional trade agreements and some specific regional data protection mechanisms.

For civil society/consumer stakeholders, *online* privacy has emerged as a very high priority issue in the area of human rights and consumer protection. Consumers International has stated that “these levels of concern are in part due to consumers’ sense that they have lost control over how data is collected and how companies utilize it once in their possession.”⁶⁸ Consumer concerns have also been fueled by the large number of high profile data breaches, and of course the revelations of widespread surveillance.

Traditional consumer protection laws are designed to protect the rights of consumers at all stages of the transaction process—from direct marketing, through to the formation of a contract, the payment process and any after-sales support. Such laws are being reformed to take into account the emergence of electronic commerce. UNCTAD undertook consultations with Member States on the revision of the United Nations Guidelines on Consumer Protection taking into account the substantive progress that has been made in other organizations, such as the OECD Guidelines for Consumer Protection in the Context of E-commerce (1999). The Guidelines were recently revised and adopted in March 2016 by the OECD Council, to reflect the developments in e-commerce since the Recommendation was first adopted. When the data generated by online activities become the product, the linkages between consumer protection and data protection policies become stronger, making it important for the regulatory regimes to support and reinforce each other to the benefit of the individual as consumer and data subject.

Consumer protection laws can invalidate certain contract terms deemed unfair to the consumer, similar to the obligation to process personal data fairly. ‘Fairness’ under both regimes is primarily achieved through the imposition of transparency obligations on the supplier or processing entity, designed to enable the individual to make informed choices. Generating security and trust amongst online users is also a shared objective, whether achieved through obligations to implement appropriate measures or through payment protection rules, minimizing a consumer’s exposure to fraud. Finally, enforcement authorities enhance national levels of compliance and through cooperative international networks can improve cross-border enforcement.

Consumers are often placed in a position where they are required to hand over personal information, in exchange for a promise that the data will only be used in a certain way. That promise may be backed up by other promises (such as a privacy trust mark, or membership of a data protection regime). Unfortunately, there is now a very visible history of significant broken promises and deception.

Some high profile examples include:

Google Streetview (various jurisdictions, 2012)⁶⁹

Google Streetview vehicles collected more than just images as they mapped the landscape. They also intercepted communications being made over private Wi-Fi networks, and although Google initially claimed that the data was ‘fragmentary’ and incomprehensible, a large number of investigators and regulators found that the data included fully identifiable personal details, including sensitive health and financial data. Google paid fines and faced other sanctions in numerous jurisdictions.

Snapchat v FTC (US, 2015)⁷⁰

Snapchat settled a case with the FTC after they were found to be misleading their consumers about a range of data practices. The key broken promise was that the messages would ‘disappear’ forever, which was in fact untrue. The FTC noted that: “If a company markets privacy and security as key selling points in pitching its service to consumers, it is critical that it keep those promises”.

FTC V TRUSTe (US, 2014)⁷¹

The FTC found that TRUSTe – a high profile provider of privacy trustmarks – was misleading consumers in several ways. This included false claims that TRUSTe was non-profit, false claims that certified companies belonged to specific data protection schemes (like the EU-U.S. Safe Harbor Framework and the COPPA Safe Harbor), and false claims that the companies were recertified each year. TRUSTe paid a U.S. \$200,000 ‘disgorgement of profits’ to settle the case.

False claims of EU-U.S. Safe Harbor Framework membership⁷²

Between 2000 and 2015 hundreds of companies falsely claimed that they were members of the EU-U.S. Safe Harbor Framework. Around 40 of these companies were prosecuted by the FTC between 2008 and 2015 following consumer complaints. Some companies were former Safe Harbor members who had failed to update their privacy policies after leaving the Safe Harbor (the record for the longest false claim is eight years). Some companies were never Safe Harbor members.

There are numerous other examples, and most broken promises do not lead to enforcement action or consumer redress. It is difficult in this environment for consumers to continue to hand over data based on ‘promises’ without any additional protection, so civil society/consumer stakeholders have a strong interest in exploring alternative forms of data protection. For example, the Consumers International contribution featured in Part II of this study states:

“It may be that new innovation will provide solutions to some of the challenges that prior innovation has created. E-commerce has a history of developing such innovative solutions, and the emergence of new personal data empowerment tools and services that return some agency over data to consumers suggests a response to data concerns that could build on regulation and legislation.”

This type of innovation also has support from some business stakeholders. For example, Microsoft has argued for the adoption of “individual empowerment” – stating that they “don’t want to negatively impact the ability to collect data. Rather, the idea is to give

individuals power in how data is used and the ability to add value to the information”.⁷³

These innovative alternatives are often categorized as privacy enhancing technologies. This is a complex field and can only be summarized briefly in this study, but some of the key examples of privacy enhancing technologies are:

Encryption

Encryption is the use of strong security measures to encode data in transit or storage (or both) so that it can only be read by the authorized user. Since the Snowden revelations in May 2013 regarding national security surveillance, there has been a ‘scramble’ for improved encryption services as a measure to protect consumers from surveillance and to win back consumer trust in using ICT services (especially cloud services). However, the use of encryption is not an absolute form of protection – there is an ongoing debate regarding the extent to which the private sector should help law enforcement agencies gain access to encrypted material.

Innovative presentation of online privacy policies

Numerous proposals and initiatives promote the development of innovative privacy policies. These include ‘short form’ privacy policies, the use of illustrations, symbols and logos, traffic light style warning systems, and others. Overall, general understanding of lengthy privacy policies is very limited, since user comprehension is poor. However, no suitable alternative has yet gained sufficient support or momentum.

Privacy seals

There was strong initial interest in the use of privacy seals or trustmarks, as a mechanism for improving privacy practices and highlighting those companies that had been certified as providing a higher level of privacy protection. However, the history of seals and trustmarks has been deteriorating over time. For example, many trustmarks no longer provide public lists of their members and/or working verification inks. Several trustmarks providers have simply disappeared. There have also been substantial issues with seal fraud. However, in recent years the U.S. Federal Trade Commission has taken an interest

in improving the quality of trustmarks, taking significant legal action against TRUSTe in 2014 (including issuing a \$200,000 fine for misleading conduct). There are also new initiatives for higher quality privacy seals in both the UK and the EU.

These various technical initiatives have struggled to provide adequate data protection in jurisdictions where the underlying privacy laws are weak. They

are best seen as a potential *complement* to baseline data protection legislation, rather than an alternative solution.

Ultimately none of these approaches has been successful (to date) and consumer stakeholders have resorted to lobbying and campaigning for regulation and strong enforcement, rather than stand-alone technical solutions.

NOTES

⁶⁴ European Centre for International Political Economy (ECIPE) for the U.S. Chamber of Commerce, The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

⁶⁵ See: <https://www.reformgovernmentsurveillance.com/>

⁶⁶ See for example the work of the Information Technology Industry Council (ITI) and Software & Information Industry Association (SIIA), <https://www.itic.org/news-events/news-releases/tech-industry-warns-president-of-risks-in-compromising-encryption>

⁶⁷ Sidley, Essentially Equivalent study - A comparison of the legal orders for privacy and data protection in the European Union and United States, (2016), p.21, <http://www.sidley.com/~media/publications/essentially-equivalent---final.pdf>

⁶⁸ See the contribution by Consumers International in Part II.

⁶⁹ Electronic Privacy Information Centre (EPIC), An Overview of Google Streetview Investigations, <https://epic.org/privacy/streetview/>

⁷⁰ FTC v Snapchat, United States, 2014, <https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were>

⁷¹ FTC v TRUSTe (United States, 2015), <https://www.ftc.gov/system/files/documents/cases/150318trust-ecmpt.pdf>

⁷² See for example: <https://www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed>

⁷³ See the contribution by Microsoft study in Part II.

CHAPTER 6: Conclusions



This study has summarized the importance of managing data protection in the context of international trade, and the diverging global, regional and national approaches to data protection regulation.

This study recognizes that there are various concerns about data protection and privacy - from consumers (civil society), businesses and governments. The challenge for data protection and privacy laws is therefore to balance these different concerns and interests, ideally in a way that does not unnecessarily hamper the scope for commerce. In order to facilitate cross-border trade online, it is also essential to seek solutions that are internationally compatible. As shown in this study, the current system is not satisfactory, and the situation needs urgently to be addressed in view of the growing economic and social activity on the Internet, and the introduction of new technologies.

It is against this background that this study has taken stock of the current situation and tried to identify possible ways forward towards a system that provides an appropriate balance between data protection and data flows.

The key findings of the study are:

There is a recognized set of core data protection principles

While there exists a remarkable degree of harmonization and coherence around the data protection core principles in key international and regional agreements and guidelines, there are diverging implementation practices.

Although there is significant divergence in the detailed data protection laws of the world, there is greater consensus around the core set of data protection principles at the heart of most national laws and international regimes.

Some data protection regimes apply equally to all those processing personal data.⁷⁴ Other regimes apply different rules to specified sectors (e.g. health industry⁷⁵), types of processing entity (e.g. public authorities⁷⁶) or categories of data (e.g. data about children).⁷⁷

A distinction can also be made between regimes that operate primarily through enforcement actions brought by individuals, or their representative groups, and those that grant enforcement powers to a spe-

cialized supervisory authority, which exercises ongoing oversight over the conduct of those that process personal data.

These core principles are:

1. Openness:
Organizations must be open about their personal data practices.
2. Collection limitation
Collection of personal data must be limited, lawful and fair, usually with knowledge and/or consent.
3. Purpose specification
The purpose of collection and disclosure must be specified at the time of collection.
4. Use limitation
Use or disclosure must be limited to specific purposes or closely related purposes.
5. Security
Personal data must be subject to appropriate security safeguards.
6. Data quality
Personal data must be relevant, accurate and up-to-date.
7. Access and correction
Data subjects must have appropriate rights to access and correct their personal data.
8. Accountability
Data controllers must take responsibility for ensuring compliance with the data protection principles.

These eight principles appear in some form in all of the key international and regional agreements and guidelines regarding data protection.⁷⁸

An additional principle – data minimization – only appears in the EU Data Protection Directive (and soon the EU General Data Protection Regulation), but that has considerable global influence.

This set of eight core principles is a useful starting point for compatibility and harmonization efforts. Countries that do not yet have laws in place, or countries that are updating or reforming their laws, should look to include the core principles in their new/amended legislation. While conformity of principles may not ensure complete mutual recognition, it may significantly contribute to policy compatibility.⁷⁹

Figure 5: Data protection core principles



Source: UNCTAD

There is a common global goal of ensuring compatibility in data protection regulation

Although numerous attempts have been made to promote global harmonization, there is no single agreed model for data protection law at this stage. However, compatibility is the stated objective of many initiatives (for example, those that have been led by the APEC, the Council of Europe, the EU and the OECD). However, no single initiative has won comprehensive global support.

Some individual countries have amended their laws to improve compatibility. New Zealand and the United States have changed their laws to ensure that foreign

citizens have data protection and dispute resolution rights (prompted in both cases by a desire to achieve compatibility and to smooth other areas of difference with the EU). This demonstrates that these countries see compatibility as an important objective.

Seven key challenges in achieving balanced and internationally compatible legal frameworks

Although there is a shared objective of compatibility, it has not yet been achieved in practice. There are significant challenges for compatibility to work in practice. Table 4 presents a summary of the main findings related to the identified seven key areas in this study.

Table 4. Summary of the main findings on key challenges in the development and implementation of data protection laws

Key challenges	Findings
1. Addressing gaps in coverage	<p>There is no single global agreement on data protection. The Council of Europe Convention 108 has had a significant 'real world' impact to date, and the EU Directive (soon to be upgraded to the EU GDPR) is driving international debates.</p> <p>There are three key gaps in <i>national</i> coverage:</p> <ol style="list-style-type: none"> 1. a significant number of countries have no data protection law at all; 2. a significant number of countries have only partial laws, or laws that contain broad exemptions; and 3. in some circumstances individual companies can limit the scope of their privacy promises (usually in the fine print of privacy policies). <p>Overall there is a strong consensus and agreement around the underlying principles of data protection. There is some divergence in the detailed implementation, although it is not as significant as the gaps discussed above.</p>
2. Addressing new technologies	<p>Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. The relationship between data protection and online activities changes all the time, but can be demonstrated by three recent developments:</p> <ol style="list-style-type: none"> 1. Cloud computing; 2. The Internet of Things 3. Big Data analytics <p>Each of them presents new challenges to data protection, particularly in the areas regarding the definition of 'personal data' and the management of cross-border data transfers.</p> <p>All three technologies can deliver enormous benefits but also carry risks for data subjects. The challenge for data protection regimes is in managing these risks, without restricting or eliminating the potential benefits.</p>
3. Managing cross-border data transfer restrictions	<p>International data flows are increasingly important for trade, innovation, competition and data mobility for consumers. However, there is also a general consensus that the movement of data cannot be completely unrestricted if legitimate concerns are to be addressed.</p> <p>Numerous options and arrangements are in place for managing the data flows in a way that still protects the rights of citizens. The most common mechanisms are:</p> <ul style="list-style-type: none"> • allowing one-off data transfers that meet common derogations or 'tests' (for example, requirements to fulfil a contract, emergency situations, valid law enforcement requests and others); • allowing ongoing data transfers where the target jurisdiction ensures an equivalent level of protection (this approach is used by the EU and other jurisdictions, including Israel and Japan); • allowing data transfers where the original company agrees to be held accountable for any breaches (this is an emerging approach that appears in the APEC Privacy Framework and to a limited degree in the laws of Australia and Japan); • allowing data transfers where the company is bound by a set of corporate rules that apply across all its activities (this approach is used in the EU BCRs, to some degree in the APEC CBPRs, and to a limited degree in national laws of, for example, Colombia and Japan); • allowing data transfers subject to a very specific legal agreement between jurisdictions (e.g. EU/U.S. agreements on transfer of airline passenger data and financial services data); and/or • some combination of the options above (it is common for national laws and global and regional initiatives to allow individual businesses to select a mechanism that is most appropriate for them). <p>Although these different options for enabling cross-border data transfers are widely available, they have not been universally adopted. In some jurisdictions, specific obstacles to compatibility have emerged. Significant developments include the emergence of data localization requirements in some jurisdictions (e.g. Indonesia, Russian Federation). While these localization requirements may seek to address certain concerns, they may also be incompatible with trade objectives.</p>

Key challenges	Findings
<p>4. Balancing surveillance and data protection</p>	<p>It is essential that national laws and global and regional initiatives acknowledge the existence of surveillance issues and attempt to address these issues head on. Most laws and initiatives are silent on this issue, a situation that needs to change now that the extent of surveillance has been revealed.</p> <p>There is an emerging ‘test’ for achieving a balance between data protection and surveillance. There appears to be an emerging consensus around the following key principles:</p> <ul style="list-style-type: none"> • the broad extent, scope and purpose of surveillance should be open, even if some operational details remain secret; • surveillance should be limited to specific national security and law enforcement objectives; • personal data collection during surveillance should be ‘necessary and proportionate’ to the purpose of the surveillance; • surveillance activities should be subject to strong oversight and governance; • all individual data subjects should have the right to effective dispute resolution and legal redress regarding surveillance (irrespective of their nationality); • private sector involvement in surveillance should be limited to appropriate assistance in responding to a specific request; and • private sector organizations should be able to disclose (in broad terms) the nature and frequency of request for personal data that they receive from government, law enforcement and security agencies. <p>An additional test is that surveillance requests should be ‘narrowly targeted’. This appears in only one key agreement to date, and has not achieved the consensus that exists regarding the ‘necessary and proportionate’ test. Nevertheless, this addition may be adopted more widely in the future.</p> <p>Balancing surveillance against data protection is complex and has only emerged recently as a major issue. Most laws and international agreements have not yet addressed it in detail.</p>
<p>5. Strengthening enforcement</p>	<p>There is a trend towards strengthening enforcement powers and sanctions in the data protection field. This is in response to a series of high profile privacy cases where existing regulatory powers have proved inadequate in the face of the massive scale and scope of the breaches.</p> <p>The imposition of proportionate sanctions is recognized as being important for: the target company (as a clear signal to senior management and staff regarding reform of their practices); the affected consumers (as an important form of redress for the harm they have suffered); and also as a broader deterrent to the wider industry.</p> <p>Strengthening enforcement has been a major theme in amending and updating laws (notably in Australia, the EU, Hong Kong (China) and Japan).</p>
<p>6. Determining jurisdiction</p>	<p>Determining jurisdiction has become a prominent issue in data protection regulation, partly due to the widespread data flows across borders, and partly due to the lack of a single global agreement on data protection (and the consequent fragmentation of data protection regulation).</p> <p>In the absence of an international agreement, jurisdiction law is complex and unsettled. Two cases that are currently before the courts and are receiving considerable attention are U.S. v Microsoft and Belgium v Facebook). Both may have an impact on the future process for determining jurisdiction in data protection law.</p> <p>Some recent amendment of legislation, notably Japan’s new privacy law and the EU General Data Protection Regulation, have resulted in specific provisions on jurisdiction, extending the reach of national laws through extraterritoriality provisions.</p>
<p>7. Managing the compliance burden</p>	<p>There is a risk of data protection requirements restricting opportunities for innovation, or creating unrealistic compliance burdens on business. Some data protection regulation is being criticized for being overly cumbersome or expensive to comply with, or that it creates specific compliance burdens for smaller businesses.</p> <p>Examples include:</p> <ul style="list-style-type: none"> • laws that include registration requirements, where the company has to notify the regulator of the existence of a data set; often the requirement is accompanied by a fee (these requirements appear in some but not all European national laws, with a few scattered examples in other regions); • laws that require the appointment of data protection officers (currently the subject of debate in the proposed EU General Data Protection Regulation); and • requirements to establish data centers or offices in local jurisdictions.

NOTES

⁷⁴ E.g. EU Directive 95/46/EC.

⁷⁵ E.g. the US Health Insurance Portability and Accountability Act, (HIPAA), 45 C.F.R. 160-164.

⁷⁶ E.g. Commonwealth Model Law on Privacy.

⁷⁷ E.g. the US Children's Online Privacy Protection Act, (COPPA) of 1998.

⁷⁸ The principles are chiefly drawn from the EU Data Protection Directive, the OECD Privacy Guidelines and the Council of Europe Convention 108. The 'order' and 'terminology' is a modified version of the work on this issue by Graham Greenleaf (see for example 'Standards by which to assess data privacy laws' in Greenleaf, G, *Asian Data Privacy Laws*, Oxford 2014.

⁷⁹ For more information, see the contribution from the International Chamber of Commerce in Part II.

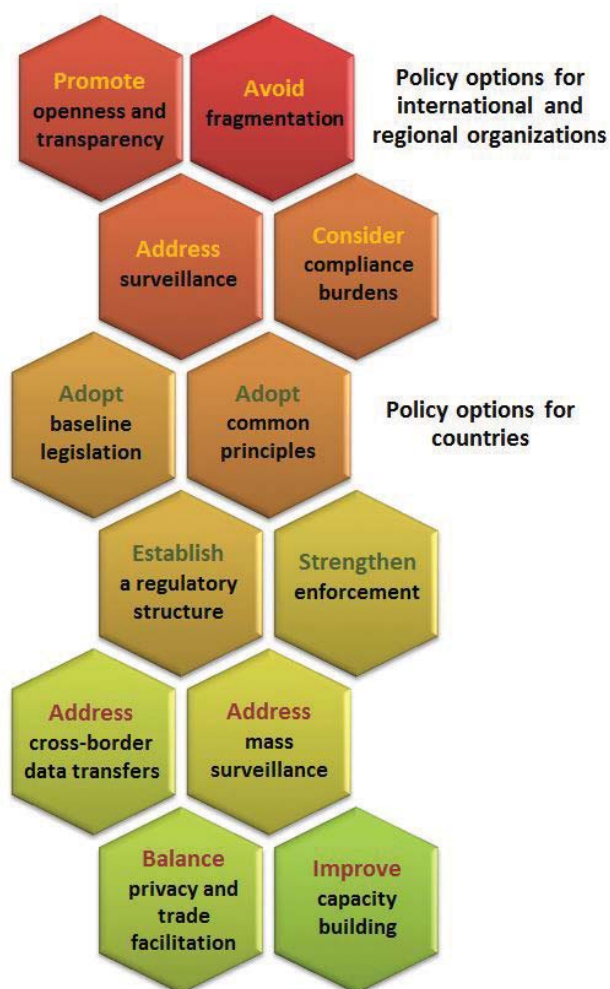
CHAPTER 7: Policy options



This chapter presents some policy options for international and regional organizations to promote compatibility, and highlights good practices for

developing, implementing and updating data protection laws in ways that promote compatibility.

Figure 6: Key Policy Options



Source: UNCTAD

POLICY OPTIONS FOR INTERNATIONAL AND REGIONAL ORGANIZATIONS

International and regional organizations have already embarked on a series of initiatives to promote data protection regulation, as summarized in this study. This section presents key policy considerations for these groups.

Avoiding fragmentation

To promote compatibility, it is important to avoid duplication and fragmentation in the regional and international approaches to data protection.

In order to promote compatibility, it is important to avoid duplication and fragmentation in the regional and international approaches to data protection.

In some other areas of law, international and regional organizations have ‘rallied around’ a single initiative to drive compatibility and harmonization. For example, in the case of cybercrime, wide support exists for the development and expansion of the Council of Europe Convention on Cybercrime 2001, which now has 54 signatories including many European countries, Australia, Canada, Japan and the US. The Convention has driven the standardization of cybercrime laws in many more countries beyond the signatory members, since the core provisions are often mirrored in national laws.

In the data protection field, by contrast, there is no single global agreement. On the contrary, there are numerous regional and international initiatives, some of which compete. While there is divergence in approach, there is quite a lot of common ground in terms of the underlying principles and a broad agreement on the concerns to be addressed.

The agreement with the broadest support, and the greatest potential for driving compatibility, is the Council of Europe Convention 108. The Convention can be signed by any country; it already has a large number of followers; it is based on broadly agreed principles; it has the support of key stakeholders (especially civil society and regulators); and its binding nature would increase compatibility. However, the Convention has yet to attract key support in North America and the Asia-Pacific.

Regardless of what instrument forms the basis of cohesion, convergence of regimes may already be taking place. As exemplified in the contribution by the European Commission, the EU intends to make strides toward internal cooperation⁸⁰:

The EU is actively involved in international cooperation on data protection through various international fora, including the OECD and the Council of Europe (and it intends to become a Party to the Council of Europe’s revised Data Protection Convention 108). The EU participates in the dialogue on privacy and data protection with regional organizations, notably with APEC.

Promoting openness and transparency

Getting the balance wrong between data protection and data flows can have serious consequences for either the protection of fundamental rights or for international trade and development.

In most cases, data protection initiatives have been developed in an open and transparent manner, with opportunities for input from a range of stakeholder perspectives. For example, the CoE Convention 108 includes a forum where national governments, regulators, private sector stakeholders and civil society representatives can all receive information and share insights on promotion and improvement of the Convention.

However, there are examples of initiatives that have been developed without the same level of input from external stakeholders. For example, international trade agreements are often seen as being developed through secretive negotiations that appear to severely limit opportunities for a consumer/civil society voice to be heard. Developing and implementing data protection law is a complex and costly process that often requires a careful balance between data protection and data flows. Getting the balance wrong can have serious consequences for either the protection of fundamental rights or for international trade and development.

Future work towards achieving greater compatibility will require the effective involvement of all stakeholders, including private sector and civil society representatives. This involvement needs to go beyond general discussions (conferences, seminars and the like) to include formal engagement in the policy development process.

The development of global and regional data protection initiatives also requires engagement with developing nations. Too often the debate is dominated by the interests of developed nations. Admittedly, the developed nations have the most mature data protection laws and the most experience in enforcing these laws, but there is growing support for improving engagement with developing countries. For example, the contribution to this report by Microsoft (see Part II) states:

The world finds itself on the leading edge of a transformative technological revolution being driven by the economic and societal benefits that derive from access to data and data analytics. Emerging Markets (EM) are racing with time to capture these benefits, but are being left out of an innovation dialogue that is largely occurring between mature markets.

Address the balance between surveillance and data protection

There is growing consensus around key conditions and limitations to address the balance between surveillance and data protection.

Most regional and global initiatives are silent on the issue of surveillance. It is essential that national laws, as well as global and regional initiatives, acknowledge the existence of surveillance issues and attempt to address these issues head on. The UN statement on digital rights sets out a platform for tackling this issue.

Addressing this balance in relation to international data flows requires appropriate conditions and limitations to be placed on surveillance, so that data controllers can allow their data to be transferred abroad with a reasonable degree of confidence.

There is growing consensus around the following key conditions and limitations:

- the broad extent, scope and purpose of surveillance should be open, even if some operational details remain secret;
- surveillance should be limited to specific national security and law enforcement objectives;
- personal data collection during surveillance should be ‘necessary and proportionate’ to the purpose of the surveillance;
- surveillance activities should be subject to strong oversight and governance;
- all individual data subjects should have the right to effective dispute resolution and legal redress regarding surveillance (irrespective of their nationality);
- private sector involvement in surveillance should be limited to appropriate assistance in responding to a specific request; and
- private sector organizations should be able to disclose (in broad terms) the nature and frequency of request for personal data that they receive from government, law enforcement and security agencies.

Consider compliance burdens

Domestic and emerging international compliance burdens put SMEs at a disadvantage and increase potential monopolization, to the benefit of larger companies.

In developing and promoting international and regional initiatives on data protection, consideration should be given to compliance burdens, and their potential impact on trade, innovation and competition, especially if smaller businesses are excluded from the initiatives. This might include conducting regulatory impact reviews on new or amended data protection legislation, and closer engagement with SME stakeholder representatives.

Most compliance burdens for smaller businesses result from domestic data protection legislation, but there are also some emerging compliance barriers in the international context. For example, there are examples of regional mechanisms for cross-border data transfers that are only used by large businesses (the EU BCRs and the APEC CBPRs), due to the high costs of application and/or annual certification. If these mechanisms act as a barrier to entry for smaller businesses this could lead to further market dominance by large, incumbent providers, reducing competition, choice and innovation.

POLICY OPTIONS FOR COUNTRIES

The number of national data protection laws has grown rapidly, but major gaps still remain. Some countries have no laws in this area, some countries have partial laws, and some countries have laws that require amendment and updating. In many countries, the first priority remains the need for awareness creation about the legal issues around data protection.

Key policy options for nations that are developing, reviewing or amending data protection laws include:

Adopting baseline legislation

Legislation should cover data held by the government and the private sector and remove exemptions to achieve greater coverage.

Countries that still do not have any data protection laws in place would need to prepare a law that should include coverage of data held by both the Government and the private sector. The law should minimize other exceptions. Recent law reviews and amendments (e.g. by Canada, the EU and Japan) have tended to remove exemptions from data protection laws in order to achieve greater coverage. There are no known examples of countries adding exemptions to their data protection laws. Although a number of countries have a sectoral approach to privacy legislation, some of these countries are in the process of drafting comprehensive laws to replace their existing patchwork of laws (e.g. India).

Adopting common principles

Adopting a core set of principles could be a way to enhance international interoperability, while still allowing some flexibility in domestic implementation.

A core set of principles appears in the vast majority of national data protection laws, as well as global and regional initiatives, referred to in Chapter 6. Adopting this core set of principles could be a way to enhance international compatibility, while still allowing some flexibility in domestic implementation.

Establishing an effective regulatory structure

The benefits of a single central regulator, especially for international trade opportunities and consumers, are considerable.

While there is divergence regarding the regulatory structure of legislation, there appears to be strong support for establishing a single central regulator when possible. Several countries have moved from a complex multi-agency regulatory structure to a simpler national agency structure (e.g. Japan has moved from 30 regulators to just one). This is not always possible due to the federated nature of the jurisdiction (e.g. Canada, Germany, and India). However, the benefits of a single regulator, especially for international trade opportunities, are considerable. Foreign companies

then only have to deal with a single point of contact, and a single regulator can drive consistency by issuing a single set of guidelines or standards. Consumers also find it easier to deal with a single regulator if they have queries or complaints, and a single consistent set of rulings and determinations by a national regulator will have more impact than a diverse set of rulings from multiple regulators.

It is important that the regulator has a complaints management role. Most regulators combine a general oversight function with this specific role, with some exceptions. For example, the FTC is a strategic regulator (it does not have to respond to individual complaints) while dispute resolution in the United States is managed in part by private litigation and third party providers. The Republic of Korea has formally ‘split’ the regulatory/complaints roles between two agencies.⁸¹

Strengthening enforcement

Enforcement powers should be proportional to the importance of data protection and the increasing size and scope of privacy breaches.

There is a strong trend towards broadening enforcement powers and increasing the size and range of fines and sanctions in data protection. This trend is evident in recent amendments to data protection laws in Australia, Japan and Hong Kong (China), and the improvements in powers and sanctions as stipulated in the EU General Data Protection Regulation.

Countries that are developing or amending data protection laws should consider taking steps to ensure that enforcement powers are proportional to the importance of data protection and the increased size and scope of privacy breaches over time. No country that has updated or amended its privacy law has so far chosen to weaken its enforcement powers or sanctions.

Addressing cross-border data transfers

Countries that are developing or amending their data protection laws need to include a specific provision on cross-border data transfers and promote one or more mechanisms that businesses can use to enable international data flows.

It is important to address the issue of cross-border data transfers by including a specific provision on cross-border data transfers and promoting one or more mechanisms that businesses can use to enable international data flows. In an increasingly globalized economy where an ever-increasing number of economic activities are undertaken online, remaining silent on the issue is not a viable option.

Current approaches to managing cross-border data transfers vary considerably. This makes it particularly important to examine possible ways to enhance compatibility in this domain. Even between developed countries there is considerable tension regarding cross-border data transfers (for example the recent court challenge to the U.S. Safe Harbor Framework in the European courts, and the introduction of data localization requirements in the Russian Federation).

Allowing a range of options for companies to consider appears to be the accepted contemporary approach to managing this issue.

Countries that are developing or amending their data protection laws may consider making some combination of the following options available, allowing:

- one-off data transfers that meet common derogations or ‘tests’ (for example, requirements to fulfil a contract, emergency situations, valid law enforcement requests etc.);
- ongoing data transfers where the target jurisdiction ensures an equivalent level of protection;
- data transfers where the original company agrees to be held accountable for any breaches; and/or
- data transfers where the company is bound by a set of corporate rules that apply across all its activities.

Balancing privacy protection against the objective of facilitating trade and innovation

Countries should strive to engage with all stakeholders and find the optimal balance between protecting data and allowing competition and innovation to thrive.

It is important for national data protection laws to avoid (or remove) clear obstacles to trade and innovation.

This may involve avoiding or removing data localization requirements that go beyond the basic options for the management of cross-border data transfers

discussed above. Examples include requirements for data to be physically located or hosted locally, requirements for establishing local company presence, and requirements for hiring local staff.

A useful test that has emerged in this area is the requirement that such provisions should not be ‘disguised restrictions on trade’. Countries may also wish to avoid/remove burdensome registration requirements from national data protection laws. This may be difficult where the registration fees help fund local regulatory activity.

Generally, countries should strive to engage with all stakeholders and find the optimal balance between protecting data and allowing competition and innovation to thrive.

Addressing mass surveillance issues

Historically, many national data protection laws have been silent on this issue, but it is now difficult to ignore the need to balance surveillance against data protection. In some jurisdictions, data protection law will be the appropriate place to address this issue. In other jurisdictions, it may be addressed through other legal arrangements.

In order to address this issue, countries need to implement measures that place appropriate limits and conditions on surveillance. Key measures that have emerged include:

- providing a right to legal redress for citizens from any country whose data is transferred into the country (and subject to surveillance);
- personal data collection during surveillance should be ‘necessary and proportionate’ to the purpose of the surveillance; and
- surveillance activities should be subject to strong oversight and governance.

Improving capacity-building options

The UN plays an important role in assisting developing countries as they develop and implement data protection laws, including research and capacity-building. For developing countries, the adoption of a data protection law is essential not only to create trust in online activities but also to ensure their effective participation in the information economy.

In this study, several contributions have stressed the importance of capacity-building for both the development of data protection laws (see for example

the contribution by Uganda in Part II) and their implementation (see for example the contribution by ECOWAS in Part II).

There are also examples of countries struggling with the enforcement of their data protection laws. In the contribution from Ghana in Part II, they note that:

“Even though the Commission has received some complaints about data breaches, enforcement actions under the Act have not been actively enforced because of the need to create awareness and also to develop the mechanisms to effectively implement enforcement actions including criminal prosecutions... There is a need to create further awareness and to build capacity among stakeholders including prosecutors and judges in order to effectively enforce applicable sanctions under the Act.”

In support of developing countries' efforts in this area, UNCTAD's E-Commerce and Law Reform

Programme assists in the preparation and revision of data protection and privacy laws aligned with international and regional instruments. The assistance provided by UNCTAD in the harmonization of e-commerce legislation across regions (ASEAN, EAC, ECOWAS, Central and Latin America) is creating an impetus for countries to push for adopting national laws in this area. UNCTAD also provides a platform for sharing best practices and experiences through its intergovernmental machinery, including those based on comparative reviews of e-commerce legislation.

Striving for balanced, flexible, and compatible data protection regulation has become an urgent goal. Some countries have powerful regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that allows for innovation and facilitates trade, it is essential to continue national, regional and global multistakeholder dialogue. International organizations such as UNCTAD could provide the platform for such dialogue.

NOTES

⁸⁰ See the contribution by the European Commission in Part II.

⁸¹ Complaints handling is managed by the Personal Information Dispute Mediation Committee (PICO), koreanlii.or.kr/w/index.php/Personal_Information_Dispute_Mediation_Committee. General policy oversight is provided by the Personal Information Protection Commission (PIPC), www.pipc.go.kr.

PART II



This part of the study presents contributions from various international and regional organizations, governments, the private sector and civil society. Each stakeholder has prepared a unique input, sharing their insights, experiences, challenges and ideas on promoting best practices in the area of data protection and privacy in the context of international trade. The views presented here are the contributors' and do not necessarily reflect the views and position of the United Nations or the United Nations Conference on Trade and Development. The contributions are organized under the following three headings: international and regional organizations, private sector and non-governmental organizations, and governments.

International and Regional Organizations

African Union Convention on Cyber-security and Personal Data Protection (AU CCPDP). Moctar Yedaly, Head, Information Society Division, Infrastructure and Energy Department, AU Commission.

Privacy Policy Developments in the Asia Pacific Economic Cooperation (APEC) Forum. Danièle Chatelois, Former Chair of the APEC Data Privacy Subgroup (2012-February 2016).

Data Protection in the Commonwealth. Elizabeth Bakibinga-Gaswaga, Legal Advisor, International Development Law, Commonwealth Secretariat.

The Council of Europe Convention 108. Maria Michaelidou, Programme Advisor, Data Protection Unit, Council of Europe.

Data Protection in the East African Community. Robert Achieng, Senior Communications Engineer, EAC Secretariat.

ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection. Dr. Isias Barreto Da Rosa, Commissioner for Telecommunication and Information Technologies, ECOWAS Commission.

Data Protection in the European Union: Today and Tomorrow. Lukasz Rozanski, Policy Officer, Data Protection, European Commission.

Private Sector and NGOs

Personal Data Protection and International Data Flows: The Case of Brazil. Rafael Zanatta, Brazilian Institute of Consumer .

Cross-border e-commerce: building consumer trust in international data flows. Liz Coll, Consumer International.

Comments of the Computer & Communications Industry Association on Data Protection Regulations and International Data Flows: Impact on Enterprises and Consumers. Bijan Madhani, Public Policy & Regulatory Counsel; Jordan Harriman, Policy Fellow, CCA.

Optimizing Societal Benefit of Emerging Technologies in Policy Development Related to Data Flows, Data Protection and Trade. Joseph Alhadeff, Chair, International Chamber of Commerce Commission on the Digital Economy; Chief Privacy Strategist and Vice President of Global Public Policy, Oracle Corporation.

Middle East and Africa (MEA) Privacy Principles Will Protect Privacy and Advance Trade, The Case for a New Legal Framework. Eduardo Ustaran, IAPP board member, Olanrewaju Fagbohun, Research Professor, Nigerian Institute of Advanced Legal Studies, Yasin Beceni, Managing Partner, BTS & Partners; and Lecturer; Istanbul Bilgi University, Ussal Sahbaz, Director, Think Tank – TEPAV, Geff Brown, Assistant General Counsel, Microsoft Corp., Marie Charlotte Roques Bonnet, Director Microsoft EMEA, Ed Britan, Attorney, Microsoft Corp., Heba Ramzy, Director Corporate Affairs, Microsoft Middle East and Africa.

Governments

The Protection of Data in Benin. Adjaigbe S. Rodolphe, Director, Studies and Research, Ministry of Communication and ICTs, Benin.

Implementation of Data Protection Legislation - The Case of Ghana. Albert Antwi-Boasiako, Founder and Principal Consultant, e-Crime Bureau, Ghana.

The Status of Data Protection in Mauritius. Ammar Oozeer, Juristconsult Chambers, Mauritius.

The Status of Data Protection in Niger. Atte Boeyi, Director of Legislation, General Secretariat; Ado Salifou Mahamane Laoualy, Director of Judicial Affairs and Litigation, Niger.

The Legal and Regulatory Regime for Data Protection and Privacy in Uganda. Denis Kibirige, Senior State Attorney, Ministry of Justice and Constitutional Affairs (MoJCA); Barbarah Imaryo, Manager, Legal Services, National Information Technology Authority (NITA-U), Uganda.

Privacy and Security of Personal Data in the United States. Staff of the Federal Trade Commission Office of International Affairs, United States.

International and Regional Organizations



African Union Convention on Cyber-security and Personal Data Protection (AU CCPDP)

Moctar Yedaly, Head, Information Society Division,
Infrastructure and Energy Department, African Union Commission.

The African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP) aims essentially at establishing a legal framework for cyber-security, electronic transactions and personal data protection. It also embodies the existing commitments of AU Member States at sub-regional, regional and international levels to build the information society in Africa by defining the objectives and broad orientations for strengthening existing legislation on information and communications technologies (ICTs) within AU Member States and within the Regional Economic Communities (RECs).

The AU Convention on Cyber-security and Personal Data Protection was adopted by the AU 23rd Assembly of Heads of State and Government, held in Malabo in June 2014. This represented the culmination of a four year process started in November 2009, when the extraordinary AU Conference of Ministers in charge of communications and information technologies was held in Johannesburg. The Ministers then adopted the Oliver Tambo Declaration, in which they “requested the African Union Commission to develop jointly with the United Nations Economic Commission for Africa, a convention on cyber legislation based on the Continent’s needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection”.

The Convention sets forth the security rules essential for establishing a credible digital space for electronic transactions, personal data protection and combating cybercrime, with a view to respecting privacy and freedoms while enhancing the promotion and development of ICTs in Member States of the African Union.

Pursuing this goal and striving to ensure proper coordination between the national, regional and global levels, lawmakers used other international instruments in the identification of best practices. For example, the Budapest Convention on Cybercrime was used as a reference for drafting the AU Convention. The AU Convention, however, aims more broadly than the Budapest Convention (e.g. inclusion of data protection).

Principles of the AU convention with regard to data protection

Most African Countries lack legislation on personal data protection (PDP). The objective of the AU Convention with regard to PDP is to establish a mechanism that shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State and the rights of local communities.

Each Member State shall commit itself to developing a legal and institutional framework for the protection of personal data and establishing the national protection authority as an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of the Convention within AU Member States.

National protection authorities shall ensure that ICTs do not constitute a threat to public freedoms and the private life of citizens by regulating the processing of data files, particularly sensitive files, and by establishing mechanisms for cooperation with the PDP authorities of third countries and participating in international negotiations on PDP.

The AU Convention aims at creating a uniform system of data processing and determines a common set of rules to govern cross-border transfer at a continental (African) level to avoid divergent regulatory approaches between the AU Member States and to ensure effective protection of personal data and the creation of a safe environment for citizens.

PDP areas covered by the Convention are:

1. any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies,
2. any processing of data relating to public security, research, criminal prosecution or State security, subject to the exceptions defined by specific provisions of other extant laws, and
3. any processing of data undertaken in the territory of a State Party of the African Union.

With the exception of some cases—private use—PDP shall be subject to a declaration and authorization to be addressed to the Data Protection Authority (DPA). The latter may establish and publish standards where it should be indicated, among other information, the identity and address of the data controller, the purpose of the processing, the origin of the personal data processed and the envisaged interconnections or transfer of these data to a third country that is not member of the AU.

In addition, processing of personal data shall be deemed legitimate where the data subject has given his/her consent. The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently. Furthermore, the collected data shall be accurate and where necessary kept up to date with respect to the principle of transparency and a mandatory disclosure of information on personal data by the data controller.

In all cases, personal data shall be processed confidentially and protected. Any natural person whose personal data are to be processed has the right of access to the information and the right to object on legitimate grounds to the processing of the data relating to him/her. Data collection shall be adequate, relevant and not excessive in relation to the purposes for which the data are collected and further processed, and the collection shall be undertaken for specific, explicit and legitimate purposes.

The data controller must take all appropriate precautions, according to the nature of the data, and in particular, to prevent such data from being altered, destroyed or accessed by unauthorized third parties. Per the convention, any interconnection between personal data files should be subject to appropriate security measures, and should also take into account the principle of relevance of the data that are to be interconnected.

1. The African Countries following the same regulatory approach

In preparing the Convention, the AU Commission, with the support of the UNECA, has not only taken into consideration the ongoing and existing cyber legislation frameworks (e.g., in ECOWAS) but has also adopted a bottom up approach in bringing experts from all concerned departments and from all AU Member States. They have provided their inputs and have been made aware of the need to consider AU regulatory framework in the preparation of their

legislation in order to prepare for the harmonization of the regulatory framework. All indicate that the approach has been adopted (e.g., ECCAS 11/11, ECOWAS 02/12, and tripartite 06/12 (East-Southern-North) validation workshops).

2. Countries in Africa facing problems of adopting laws for developing e-commerce and engaging in business relations with other countries

Given the international dimension of cybersecurity, it is important to reinforce regional and international cooperation to develop the necessary legal frameworks to fight cybercrime. In addition to the adoption of the AU Convention, considerable progress has been made in developing regional model legislations in areas related, for example, to data protection, e-transactions and cybercrime (ECOWAS Cybersecurity guidelines, ECCAS Model Law/CEMAC Directives on Cybersecurity, SADC Model Law on data protection, e-transactions and cybercrime). Nonetheless, much more remains to be done.

3. Challenges facing the ratification of the AU convention

After its adoption by the 23rd Assembly of the Heads of States and Governments, the AU Convention on Cybersecurity and Personal Data Protection is now open to all AU Member States for signature and ratification in conformity with their respective constitutional procedures. *The convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.*

During the First Ordinary Session of the Specialized Technical Committee on Communication and Information and Communication Technologies (STC-CICT-1) held in Addis Ababa in September 2015, the Ministers in charge of ICTs committed themselves “to collaborate with relevant local and international stakeholders on the Internet Governance, Cybersecurity and Cyber criminality and they tasked the African Union to ensure the follow up of the ratification of the AU Convention on Cyber-Security by Member States”.

As of March 2016, the AU had received only eight signatures by Member States of the Convention, namely: Benin, Chad, Congo, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia, and no ratification. The AU Commission shall undertake advocacy activities for the ratification. The

challenge is to have the Convention entering into force within the next two years at most.

4. Advantages and drawbacks of adopting the AU convention/electronic transaction provisions for consumers and enterprises

We live in the digital economy era with extensive use of e-transactions (eT) in all sectors of economic activity. We are already in the era of The Internet of Things (IoT) that provides unparalleled potential benefits for major enterprises, small businesses and governments. All are embracing eT/IoT. Africa must make use of this opportunity to transform itself and catch up with the developed world, especially in the areas of education, health and food production.

Since most household items are today being operated through the Internet/WIFI, consumers are concerned about the protection of their data and home network from malicious attacks such as hacking a keyless entry device, a garage door opener, or any other home system connected to WIFI.

The rapid development of IoT makes enterprises interconnect their devices in-house, hence increasing vulnerabilities to their systems. Enterprises need also to protect their sensitive information from malicious attacks.

Everyone can benefit from using eT/IoT. This is why it is more important for all to have in place the right cyberlegislation.

Cybersecurity is particularly challenging for African countries, especially due to the low level of security provisions for preventing and controlling technological and informational risks, the low level of development of the necessary cybersecurity legal framework to fight cybercrime, and the lack of human capacity and expertise, as well as financial resources to monitor and defend national networks.

The specificity of the AU Convention on Cybersecurity and Personal Data Protection makes it unique—it addresses PDP, e-transactions, cybercrime and cybersecurity in a single place. Its objectives are to define a regional harmonized framework for cybersecurity legislations, to develop general principles as specific provisions related to cyber legislations and measures required at the Member State level, and to develop general and/or specific provisions on intra-African and international cooperation related to cyber activities.

The Convention embodies all aspects of cyberspace, including the organization of e-commerce, the protection of personal data, the promotion of cybersecurity, and the fight against cybercrime. Therefore, by adopting the AU convention and transposing it into national policies, the different model laws and guidelines implemented by States will allow for the development of a more harmonized regional legal framework built on common minimum standards, principles and procedures in the regulation of cyberspace and the fight against cybercrime at continental level.

5. Harmonization of cyber legislation at regional and continental levels and the African Union support for the implementation of the Convention

African governments are at different stages of establishing policy instruments and legislative frameworks. While many countries have proposed legislation, the level of implementation of the regional model laws and deployment of security systems in both the private and the public sector remain low.

There is a growing need to elaborate further national cybersecurity frameworks, harmonized at regional level and in line with existing international standards and practices, so that trust and confidence in the use of ICTs can be facilitated at all levels.

In this regard, the AU is committed to following up on the ratification process and will assist African countries in their efforts to transpose the Cybersecurity Convention provisions into their National Laws; others can be guided by it to develop their national legislations.

The AU project on cybersecurity capacity-building includes awareness raising workshops, in-country best practices workshops, and in-country intensive human and institutional capacity-building on cybersecurity, cybercrime, e-transactions and personal data protection. Furthermore, the project will identify specific needs related to revising existing national Cybersecurity legal frameworks and developing National and Regional Computer Emergency Response Teams (CERTs/CSIRTs) to address pertinent issues. These include enforcement measures applicable to cyberthreats, collaboration and support in the identification of technical measures for effective investigation, and prosecution protocols in accordance with international practices and standards to enable and enhance international cooperation in the fight against cybercrime.

Privacy Policy Developments in the Asia Pacific Economic Cooperation (APEC) Forum

Danièle Chatelois, Former Chair of the APEC Data Privacy Subgroup (2012-February 2016)

1. Introduction

Established in 1989, the Asia Pacific Economic Cooperation (APEC) forum is composed of 21 member economies that together represent approximately 55 percent of the world's GDP, 44 percent of world trade and 41 percent of the world's population. APEC's breadth of coverage makes this forum uniquely positioned to influence the development and implementation of consistent rules for the protection of personal information throughout the Asia Pacific region.

As a multilateral economic forum dedicated to achieving free and open trade and investment, APEC focusses on three key pillars: trade and investment liberalization; business facilitation; and economic and technical cooperation.

Privacy is one of the many areas in which APEC working groups and member economies carry out their work in support of APEC's trade and investment objectives. Its work on privacy is undertaken by the APEC Data Privacy Subgroup (DPS), a sub-forum of the Electronic Commerce Steering Group (ECSG). The DPS, which is composed of representatives of all APEC member economies, as well as APEC guest organizations, engages in the development and implementation of initiatives that provide effective and meaningful protection for personal information, which is essential to the development and maintenance of trust and confidence in the digital marketplace.

By encouraging APEC member economies to implement privacy laws and/or policies based on the minimum standards set out in the APEC Privacy Principles, the DPS contributes to the establishment of a legal and policy environment within the APEC region that is consistent, predictable and supportive of the free flow of information across borders. This approach is intended to provide legal certainty and clarity for businesses and individuals alike. Consistent regulatory frameworks reduce costs and administrative burdens for companies and consumers by minimizing conflicting legal requirements and helping to avoid barriers to information-based activities.

APEC member economies implement APEC initiatives on a voluntary basis. APEC is not a treaty

organization and APEC does not impose legally binding arrangements or treaty obligations on APEC member economies. As a result, APEC does not impose obligations on its member economies with respect to privacy legislation, regulations or policies. Rather, to guide the development of consistent domestic and international privacy approaches in the APEC region, the DPS has developed a commonly agreed upon set of APEC Privacy Principles for the protection of personal information. Meant to benefit both the economies in developing laws and companies implementing policies and practices, the Principles are found in the APEC Privacy Framework and comprise nine principles for the protection of personal information that were endorsed by APEC ministers in 2005. The APEC Privacy Framework was developed to:

- develop appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
- recognize that the free flow of information is essential for both developed and developing market economies to sustain economic and social growth;
- enable global organizations that collect, access, use or process data in APEC economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- assist enforcement agencies in fulfilling their mandate to protect information privacy; and
- advance international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

The APEC Privacy Principles (and a commentary upon the Principles) are the core of the APEC Privacy Framework. However, the Framework also contains guidance for domestic and international implementation of the principles. With respect to international implementation, the Framework includes guidance on information sharing among member economies, cross-border cooperation in investigation and enforcement, as well as on the cooperative development of cross-border privacy rules.

The DPS has proposed some updates to the APEC Privacy Framework, to mark the Framework's 10th anniversary. Given that the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were the foundation and starting point for developing the APEC Privacy Framework, the DPS in [2015] decided that updates to the Framework should be based on an understanding and consideration of changes to the OECD Guidelines made in 2013. The changes modernized and supplemented the OECD Guidelines, to make them more effective for the changed technological and business environment, while maintaining the 1980 principles unchanged and basic structure of the Guidelines intact. A comparative review of the 2013 changes to the OECD Guidelines with the APEC Framework identified a number of areas where the APEC Framework could benefit from updating.

Proposed adjustments to the APEC Privacy Framework include recommended additions to the domestic and international implementation sections, such as incorporating the concept and elements of a privacy management programme, adding data breach notification, text promoting interoperability and internationally comparable metrics. Adjustment should also include guidance for establishing privacy enforcement authorities, in particular, their role their attributes and support needed for such authorities. As with the changes to the OECD Guidelines, the Framework Principles are being left intact. The updates to the Framework continue to be considered by the APEC Electronic Commerce Steering Group (ECSG) following the first Senior Official Meetings of 2016, which were held in Lima, Peru in February. In the meantime, the DPS has undertaken various initiatives in support of the proposed additions to the Framework and will continue to explore opportunities for future work.

2. Cooperative Development of Cross-Border Privacy Rules

The APEC Privacy Framework calls for the development of a system of voluntary cross-border privacy rules for the APEC region. More precisely, it commits member economies to support the development and recognition of organizations' cross-border privacy rules across the APEC region. These rules and associated mechanisms should facilitate responsible and accountable cross-border data transfers, as well as effective privacy protections, without creating unnecessary barriers to cross-border information

flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

In accordance with this guidance, the APEC Framework was used to form the basis of an APEC-wide mechanism that confirms a baseline level of privacy protection and facilitates transfers of personal information across the APEC region. This mechanism, referred to as the "Cross-Border Privacy Rules (CBPR) System" is a privacy seal that, through the use of an independent certifying body (accountability agent), verifies and certifies that companies' information handling policies and practices are compliant with the APEC Privacy Framework Principles. The CBPR System also establishes a dispute resolution mechanism for individuals and participating companies and provides backstop enforcement through each participating economy's Privacy Enforcement Authority.

A mechanism such as the CBPR System, whereby organizations demonstrate that they comply with an internationally agreed upon set of privacy rules, represents an important element of a policy and legal environment that provides meaningful protection for personal information and that builds trust and confidence in the online marketplace. As well, the CBPR system facilitates and puts privacy interoperability into practice by bridging across the various privacy regimes that are in place in the region. The CBPR System is designed to work with domestic privacy laws. It does not displace or supplant them. Rather, it helps APEC privacy regimes work together and increases their compatibility.

The features of the system, which allows a multitude of actors to play a role and achieve privacy results, combined with the flexibility of these elements, allow economies latitude in how they meet the CBPR System program requirements.

The certification process itself is inherently flexible. For instance, an economy and its Accountability Agent may certify participating companies using program requirements that are based on a domestic law, to the extent that they have demonstrated that they meet or exceed those in the CBPR System. In such an instance, a CBPR certification would demonstrate that companies certified against the domestic privacy requirement also meet the APEC-wide baseline standard.

Another important element of interoperability is demonstrated through the enforcement aspects of the System. For instance, member economies

may only participate in the CBPR system if their Privacy Enforcement Authority (PEA) is a participant in the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), a collaboration facilitation framework for privacy enforcement. This ensures that PEAs are able to take enforcement action under their own domestic laws, to the extent that they have the effect of protecting personal information consistent with the CBPR System program requirements. At the same time, participation in the CPEA directly furthers objectives related to interoperability, because enforcement cooperation is an essential ingredient of regulatory and economic integration.

The ability of organizations to proactively demonstrate privacy compliance was recently further enhanced by the development of the APEC Privacy Recognition for Processors (PRP) System. Finalized in August 2015, the PRP System is designed to help personal information processors demonstrate their ability to assist controllers in complying with privacy obligations. The PRP also helps controllers identify qualified and accountable processors. As under the CBPR System, the PRP System relies on an independent Accountability Agent to verify and certify that processors' information handling policies and practices are compliant with a set of baseline privacy requirements. The PRP also provides a dispute resolution mechanism for individuals, controllers and processors, as well as backstop enforcement through each participating economy's PEA.

3. APEC and EU Interoperability

As generally acknowledged in the digital age, information may flow without regard for domestic or regional boundaries. As a result, companies that have had their privacy policies and practices certified under the CBPR system are likely to be subject to privacy laws and regulations of jurisdictions outside of the Asia Pacific.

The APEC CBPR and PRP Systems primarily facilitate responsible and accountable transfers of information within the APEC region. To further enhance support for cross-border information flows and reduce the administrative efforts associated with multiple-party regional privacy compliance, the DPS joined forces with the EU Article 29 Working Party to create a Joint EU/APEC BCR-CBPR Working Team and develop an APEC/EU Referential for the structure of the EU Binding Corporate Rules (BCR) and APEC CBPR System, (aka "Common Referential").

The Common Referential, released in March 2014, is a concrete example of pragmatic tools to help bridge privacy protection systems, in support of interoperability. It aims to assist organizations in understanding and complying with the requirements of both the CBPR and the BCR Systems. While not intended to constitute mutual recognition between the two, the Common Referential is envisioned as a high level guide and a pragmatic reference for companies, to facilitate their implementation of BCR/CBPR compliant policies and practices and to help them identify additional compliance requirements where appropriate.

Following the release of the Common Referential, the Joint Working Team agreed to explore further the development of additional tools to complement the Common Referential, as well as to assist with and expedite compliance with both systems. In response to an expression of interest by the APEC Data Privacy Subgroup, the Article 29 Working Party agreed to, in the short to medium term, a common application form to facilitate double certification and a mapping of company policies, practices and tools to be submitted along with the common questionnaire and—in the longer term—a Common Referential for the EU Processor BCRs and APEC PRP System. Work on the common questionnaire commenced at the August 2015 APEC meetings held in Cebu City, Philippines.

Such efforts in support of interoperability between APEC and EU privacy instruments are particularly pertinent in light of the new EU General Data Protection Regulation (GDPR). These efforts show promise, since they may offer continued opportunities to develop additional tools in support of interoperability between APEC mechanisms and those newly established or recognized under the GDPR with respect to transfers of personal information.

APEC Leaders and Ministers, who annually set the vision for overarching APEC goals and initiatives, provided further encouragement for the work of the DPS in 2015. In their Joint Statement issued at the conclusion of the 2015 APEC meetings, Trade Ministers acknowledged the importance of the APEC CBPR System in facilitating trade, and welcomed the increased participation of APEC economies. This recognition was further enhanced by the APEC Leaders' own commitment to promote cross-border privacy and to protect consumer interests, which they made in their 2015 Declaration. In their 2011 Declaration, APEC Leaders had already committed

to implementing the CBPR System to reduce barriers to information flows, enhance consumer privacy, and promote interoperability across regional data privacy regimes. Together, these commitments provide clear direction and ongoing support for the continued efforts of the DPS to build trust and confidence in

the digital economy, facilitate the establishment of meaningful, consistent rules for the protection of personal information and reduce impediments to cross-border flows of personal information in support of trade and investment.

Data Protection in the Commonwealth

Elizabeth Bakibinga-Gaswaga, Legal Adviser, International Development Law, Commonwealth Secretariat

1. Introduction

Personal information is a significant component of trade and business in today's data-driven economy. For a fragmented and geographically dispersed global value chain⁸² to function, large quantities of digitized information and data must be moved, often across national borders.⁸³ The Commonwealth seeks to ensure that its members, in particular from Africa, the Caribbean and Pacific regions benefit from such global value chains.⁸⁴

Commonwealth jurisdictions, most especially Small Island and Developing States that do not have adequate laws and policies for data protection, and in particular cross-border flow of personal data, may not benefit from this global value chain to the extent that they otherwise might.

The Commonwealth Secretariat has contributed to the development of data protection regimes around the world, in particular through the influence of Commonwealth model laws on national legislation of member countries. Whilst progress has been made, the state of data protection laws across the Commonwealth nonetheless varies from state to state. Jurisdictions such as Australia, Canada, New Zealand and the United Kingdom, as members of the Organization for Economic Cooperation and Development (OECD), have developed advanced data protection regimes in line with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.⁸⁵ As members of the European Union, Cyprus, Malta and United Kingdom are bound by the EU Data Protection Directive.⁸⁶ Australia, Brunei Darussalam, Canada, Hong Kong, Malaysia, New Zealand, Papua New Guinea and Singapore are members of the Asia-Pacific Economic Cooperation (APEC) which has a privacy framework in place.⁸⁷ Commonwealth jurisdictions in Africa, the Americas, Asia and the Pacific benefit from a number of regional regimes and guidelines.⁸⁸ However, data protection law in a number of large Commonwealth countries, such as India, Nigeria and South Africa, remains in the process of development. Some small Commonwealth States such as the Bahamas, Lesotho, Mauritius and Trinidad and Tobago have data protection legislation

while others, such as Guyana, Botswana and all small Commonwealth states in Asia and the Pacific,⁸⁹ have not enacted comprehensive data protection laws.

2. The Commonwealth regime

Whilst the majority of Commonwealth countries share a legal tradition of common law, there is no binding legal regime applicable to all Commonwealth jurisdictions. In each of the 53 member countries, data protection is regulated by domestic laws, mainly constitutional and statutory law provisions, as well as common law principles. In some instances, regulatory regimes imposed by regional bodies such as the European Union are also applicable. The Commonwealth Secretariat provides technical assistance to member countries in response to requests, especially least developed states, small states and vulnerable states, showing sensitivity to their unique challenges concerning legislation, policy, resource and capacity needs, among others.⁹⁰

Commonwealth Law Ministers have recognized the fundamental importance both of the right of the public to access information held by government (in the form of freedom of information laws), as well as a need to protect the privacy of individuals whose personal information is held by a government or public institution (in the form of informational privacy and data protection guarantees).⁹¹ In response to requests from Law Ministers, the work of the Commonwealth Secretariat has focused on, among others, providing a model legal framework to member countries for control over collection, access to, use of, and dissemination of data stored in digital and in paper-based systems.

In 1999, Law Ministers endorsed the *Commonwealth Freedom of Information Principles*, which were subsequently noted by the Commonwealth Heads of Government (CHOGM) at their Durban Meeting in 1999.⁹² CHOGM recognized the importance of public access to official information, both in promoting transparency and accountable governance and in encouraging the full participation of citizens in the democratic process. The basis of the *Commonwealth Freedom of Information Principles* is the *Declaration of Commonwealth Singapore Principles, 1971*, which recognizes the liberty of the individual and to that end

strives to promote in each of the member countries guarantees for personal freedom under the law.⁹³

The recognition by the Commonwealth of the potentially conflicting rights to access to information and to privacy have led to the development of various initiatives. These initiatives unfolded in three dimensions: the development of model laws on the protection of personal information; the regulation of information privacy including freedom of information; and the establishment of mechanisms to combat cybercrime, including crimes that affect informational privacy.

Data breach—the access, viewing, interception or use by an individual unauthorized to do so of sensitive, protected or confidential data—form the *actus reus* of a number of cybercrimes such as Internet fraud, identity theft, and credit card account thefts. Measures to safeguard against cybercrime affect the increased cost of doing business due to: expenses incurred in identifying risks, building new and more secure procedures, and buying and maintaining protective software and hardware; lost sales as business operations are shut down to address breaches; and expenses for investment in more advanced data protection systems.⁹⁴ The sheer volume of electronic data means that data processing and protection rules originally designed with paper-based systems in mind are also now supplemented by cybersecurity standards designed to reduce the risk of fraud, theft of sensitive data and other related cybercrimes. Commonwealth initiatives have sought to provide legislative frameworks to address the protection of personal information through data protection, information security and cybercrime prevention approaches. The Commonwealth's three-dimensional approach addresses frameworks for cybersecurity, the update of data protection legislation (in particular the understanding of personal data in a cyber-environment), and the adoption of a core periphery approach to human rights (balancing access to information with the protection of informational privacy).⁹⁵

Commonwealth Model Laws on Privacy and Data Protection

In 2002, Law Ministers considered three interrelated model Bills on privacy and freedom of information namely: the Freedom of Information Bill; the Privacy Bill; and the Protection of Personal Information Bill to

assist member countries that had yet to enact laws providing for access to, processing and protection of information.⁹⁶

Drawing largely from the OECD Guidelines, the core principles of the Commonwealth model laws are: right of access to information in documentary form in the possession of public authorities with established exceptions; recognition of the privacy of individuals by protecting personal information processed by private organizations; accuracy and security of information; involvement of the data subject; and limits to collection, use, retention and disclosure of personal information. Critical to note, the Commonwealth model laws on privacy and data protection do not include provisions for cross-border data transfers. This represents a significant shortcoming in light of the importance of such transfers to global digital trade, and represents one possible area for future review and possible revision of the model laws.

Model Protection of Personal Information Bill

The increased dependence on the Internet for business and communication has led to both public and private sectors processing significant amounts of personal information. As a result, the Secretariat prepared for consideration, a *Protection of Personal Information Model Bill*, with a particular focus on the processing of personal information by private organizations. Taking into consideration the application of related legislation in developing Commonwealth states, and also the level of advancement of technology in many of these countries, the Bill provides for the recognition of the privacy of individuals by regulating the processing of personal information or data by private sector organizations. It does not apply to public authorities or to information processed for personal or domestic, journalistic, artistic or literary purposes.

The model Bill embodies core principles of data protection. These include: setting limits on the collection of personal information or data; restricting the use of personal information or data for openly specified purposes; ensuring the right of individual access to personal information relating to that individual and the right to have it corrected, if necessary; and identifying the parties who are responsible for compliance with the relevant data protection principles. The Protection of Personal Information Bill allows for the processing of personal information; requires appropriateness of purpose, knowledge and consent; and sets limits and conditions on use and disclosure of personal

information within and outside the given member country. The Bill requires role occupants to ensure accuracy of the information; to secure personal information; to retain records and note all uses and disclosures without consent. The Bill also regulates the procedure for access to information, including the process for persons with disabilities, and the manner in which complaints are received, investigated and disputes resolved. The role of a Privacy Commissioner is also set out, including the requirement to make an annual report to Parliament. The Bill regulates cross-border disclosures of information, requiring guarantees of protection.

In light of the fact that some developing Commonwealth states may face challenges in securing adequate resources for an independent body or authority to deal with complaints under the legislation, provision was also made for the Privacy Commissioner appointed under the Privacy Act (dealing with the protection of personal information in the public sector) to also deal with complaints under the Protection of Personal Information Bill. References to the Commissioner in provisions were square bracketed, with the intention that they could be replaced by references to an alternate appropriate official, such as an ombudsman.

Model Privacy Bill

The Commonwealth Model Privacy Bill aims to provide a model framework for protection of personal information held by public bodies, through ensuring that information is collected only for appropriate purposes and by appropriate means. The model Privacy Bill sought to affirm the OECD principles and to create a legal regime that could be administered by small and developing States without the need to create significant new structures. The Bill: provides for the collection, use, storage, security, disclosure and retention of personal information by public authorities; creates the office of Privacy Commissioner; and provides for investigation of complaints and accountability to Parliament. Provisions dealing with the creation of a Privacy Commissioner are included on an optional basis, with a view to assisting small and developing States that may not be able to create such an office and instead rely on courts or tribunals to deal with allegations of damage caused by breach of the privacy law. In the absence of resources to create the office of a Privacy Commissioner, another officer could be designated to perform certain critical functions relating to protection of personal privacy.

Model Freedom of Information Bill

The Model Freedom of Information Bill was prepared to assist those countries desiring to affirm the *Commonwealth Freedom of Information Principles*. While creating a right of members of the public to access information held by public authorities with the aim of increasing transparency and accountability of government, the model Bill creates exemptions in the interest of privacy. Documents, disclosure of which would involve unreasonable disclosure of personal information of any individual, are exempted from disclosure. This provision adds an additional layer of protection of personal information.

3. *Data Protection laws across the Commonwealth*

Diversity amongst the 53 independent countries of the Commonwealth, which include large and small, developed and developing, landlocked and island economies, presents certain challenges to a 'one size fits all approach' to data protection laws. Rather, the Commonwealth approach is guided by the principle of 'best fit' rather than 'best practice' and is flexible—as well as culturally and contextually sensitive—and emphasizes country ownership.⁹⁷ Individual member countries are therefore free to make use of the Commonwealth model laws as they deem fit, and the uptake of draft model laws and guidelines is dependent upon their needs. Before endorsing the Commonwealth model laws, Law Ministers were cognizant of the fact that some member countries face resource challenges and are not necessarily in position to establish institutional frameworks to solely take responsibility for data protection. To that effect Law Ministers recommended flexibility regarding the adoption of the relevant provisions.

Across the Commonwealth, the membership of regional bodies has a significant influence on data protection laws. With respect to cross-border transfers of data, for example, Cyprus, Malta and the United Kingdom are subject to European legislation and practice, whilst Canada, Hong Kong, New Zealand, SAR China and Singapore, are participants in the APEC Cross-border Privacy Enforcement Arrangement, which aims to facilitate both domestic and international efforts to promote and enforce information privacy protections.⁹⁸ Examples of regional developments that affect policy and legislative developments in Commonwealth Member States

also include current initiatives by the International Telecommunications Union (ITU),⁹⁹ United Nations Economic Commission for Africa (UNECA)¹⁰⁰, the African Union,¹⁰¹ and the Pacific Island States.¹⁰²

National laws relating to privacy in general and data protection specifically are contained in some instances in structured comprehensive data protection laws, fragmented sectoral laws, self-regulatory codes of conduct, criminal law, common law and through enforcement of contractual obligations. One common standard is where privacy and information is protected under the common law doctrines of the duty of confidentiality, the recognition of individual's rights in personal information and the recognition of privacy as a human right under provisions of national constitutions.

Member countries and their national experiences remain diverse. Small Island Developing States, such as the Bahamas, have their own peculiar vulnerabilities and characteristics such as their small size, remoteness, narrow resource and export base, and exposure to global environmental challenges and external economic shocks.¹⁰³ Canada and the United Kingdom represent high income developed economies.¹⁰⁴ On the other hand, South Africa represents upper middle income developing economies while India and Nigeria represent lower middle income developing economies.¹⁰⁵

There is a large range of degree of protection across the Commonwealth, with some countries such as the Bahamas, Canada and the United Kingdom, regardless of the level of income, having very advanced and comprehensive data protection laws, while others have legislation under development, and some, especially in the Asia-Pacific region, have none at all. In some instances, sectoral legislation provides some protection to informational privacy.

Where there are laws, there is variance in the modalities contained in national legislation but overall, the guarantees set out in the broader common frameworks such as the principles of data protection set out in the OECD Guidelines and internationally accepted best practices are provided expressly or by

implication. It is clear that while there are similarities in regulatory approaches to data protection, there cannot be said to be a harmonized data protection regime across the Commonwealth. Whilst the Commonwealth model laws have played an important part in the inclusion of key principles within national data protection laws, further work is required in order to obtain a comprehensive picture of their exact degree of implementation across the 53 countries.

It is possible that the lack of a harmonized approach to data protection may present challenges to some aspects of international trade and supply of goods and services, mainly through legislative or contractual limitations to transborder data flows to countries with less well developed data protection regimes. Further harmonization of laws across the Commonwealth could facilitate cross-border data movement, with countries more able to guarantee to each other equivalent protections. The 53 Commonwealth members' combined exports of goods and services were valued at \$3.4 trillion in 2013, which is about 15 percent of the world's total exports, with expectations of increasing intra-Commonwealth trade from \$592 billion in 2013 to \$1 trillion by 2020.¹⁰⁶

In order to keep up with developments in information and communication technology, and changing business models and regulatory frameworks, further research is required on such questions as: the implications of the increasingly interlocking data export restrictions in legislation; the effectiveness of the enforcement regimes in various countries; the extent of judicial interpretation of laws, and other comparative aspects of data privacy laws. A decade after the Commonwealth model laws on personal information and privacy were adopted, a possible review of the laws could include an assessment to establish their impact on member countries or trade impact on consumers and enterprises in member countries as a result of non-compliance with data protection regulations in general. The costs and benefits to consumers and enterprises in member countries following the uptake of Commonwealth model legislation, as well as compliance and impacts of non-compliance should also be examined.

The Council of Europe Convention 108

Maria Michaelidou, Programme Advisor, Data Protection Unit

1. Short background on the Convention and additional protocols

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms enshrines the right to respect for private and family life. However, it rapidly became apparent that in order to fully protect individuals, a more specific protective system was needed; one that would not just contribute to the exercise of the right to private life. The system would also enable the enjoyment of other human rights and fundamental freedoms such as, the freedom of thought (Article 9), the freedom of expression (Article 10) and the freedom of assembly and association (Article 11).

From the beginning of the 1960s, rapid progress in the field of electronic data processing and the first appearance of mainframe computers allowed public administrations and big enterprises to set up extensive data banks and to improve and increase the collection, processing and interlinking of personal data. While this development offered considerable advantages in terms of efficiency and productivity, in return it gave rise to a trend of increasing electronic storage of data concerning individuals. Thus, the Council of Europe decided to establish a framework of specific principles and norms to prevent unfair collection and processing of personal data.

A first step in this direction was taken in 1973 and 1974, with the adoption of Resolutions (73) 22 and (74) 29, which established principles for the protection of personal data in automated data banks in the private and public sectors. The objective was to set in motion the development of national legislation based on these resolutions. However, during the preparation of these texts it became apparent that comprehensive protection of personal data would be effective only through further reinforcement of such national rules by means of binding international norms. The same suggestion was made at the Conference of European Ministers of Justice in 1972.

In 1981, after five years of negotiation, the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) was open for signature on 28 January, the date on which we now celebrate Data Protection Day.

It is still to date the only international legally binding instrument in the field, and is open for accession to any country across the globe. Under the Convention, the Parties are required to take the necessary measures in their domestic legislation to apply the data protection principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

This Convention was subsequently supplemented by an Additional Protocol in 2001. Taking into account the increase in exchanges of personal data across national borders, it became necessary to ensure the effective protection of the right to privacy in relation to the transborder flow of personal data. The Additional Protocol further requires Parties to set up supervisory authorities, exercising their functions in complete independence, and giving them powers of investigation and intervention, as well as the power to engage in legal proceedings.

Modernization

On the 30th anniversary of the Convention in 2011, the time was suitable for re-thinking its protection system in order to ensure its efficiency for the next thirty years.

The main objectives of the modernization are to tackle the challenges to human rights and fundamental freedoms posed by new technologies and practices of information society, while maintaining the Convention's advantages, i.e. it's generally open and technologically neutral nature (supplemented by sectoral recommendations e.g. police, employment, biometrics, medical data and profiling). Another efficiency enhancement of the Convention is the power to assess the compliance with the Convention's principles by the Parties: the evaluation and follow-up mechanism.

The overall aim is to pursue the global promotion of a set of fundamental principles that could be applied by as many countries as possible, in order to assure the protection of individuals' personal data.

2. Main principles and link to the EU data protection directive (revision process)

Convention 108 protects the individual against abuses that may accompany the processing of personal data

and seeks to regulate at the same time the transborder flow of personal data.

As regards the processing of personal data, the principles laid down in the Convention concern, in particular, fair and lawful collection and automatic processing of data, storage for specified legitimate purposes and not for ends incompatible with these purposes, nor kept for longer than necessary. They also concern the quality of the data, which must be adequate, relevant, not excessive (proportionality), and accurate. In addition, the principles include data subjects' right of access and right to rectification.

In addition to providing guarantees for processing personal data, it outlaws the processing of "sensitive" data about a person's race, politics, health, religion, sexual life and criminal record, in the absence of proper legal safeguards.

The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Moreover, security measures should be put in place, taking into account the degree of vulnerability, the need to restrict access to the information within the organization and requirements concerning long-term storage.

Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

While the Convention provides for free flow of personal data between states that are party to the Convention, it also imposes some restrictions on transborder flows of personal data to states where equivalent protection is afforded. Article 2 of the Additional Protocol to Convention 108 establishes the principle that transborder flows of data to a recipient that is not under the jurisdiction of a Party to Convention 108 are subject to the condition of an adequate level of protection in the recipient country or organization. However, Parties to Convention 108 can determine exemptions from the principle of an adequate level of protection. One of these exemptions concerns the provision of safeguards by the controller responsible for the transfer, and can in particular result from contractual clauses approved by the competent supervisory authority. Exemptions are also possible if domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests.

The consistency of the Convention with other legal frameworks also has to be safeguarded, for instance with the data protection framework of the European Union, which is currently being reviewed. Directive 95/46/EC gives substance and amplifies the principles of Convention 108 (see Recital 11 of the Directive) and while the frameworks are very different in nature and objectives, they will continue to complement each other in order to enhance the protection of individuals.

This consistency is maintained in the EU Draft Regulation. While the text is still in negotiation, it is important to note that the Council of the European Union has proposed that Recital 81a of the draft regulation makes a clear reference to Convention 108 when assessing the adequacy of the level of protection, providing that "...in particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account." [General approach adopted on 15/6/2015]

Similar links prevailed when the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted in 1980, and cooperation between the institutions continued, for instance in reviewing the Guidelines, providing valuable contributions not only to maintain compatibility among both instruments, but also steering global discussions on the topic.

3. Number of parties to the Convention

The Convention currently applies to 47 State parties (September 2015). Forty-six of the 47 Member States of the Council of Europe ratified the Convention, except Turkey.

With regards to non-members States of the Council of Europe, Uruguay was the first non-European country to become party to the Convention in 2013. Three other countries were invited to accede to the Convention and its additional Protocol (Morocco, Mauritius and Senegal); they are currently in various stages of this process. In August 2015, Tunisia expressed an interest in acceding.

4. Challenges countries encounter in the implementation of the Convention

In its current form, Convention 108 does not provide for a follow-up mechanism enabling the identification of challenges that countries encounter during its

implementation. This will be reconciled when the modernized convention is adopted. In this regard, the Convention Committee will have two new functions:

- To evaluate a candidate for accession in terms of the guaranteed level of protection and its conformity with the Convention;
- To follow-up the implementation of the Convention by a Party to the Convention.

In relation to the follow-up process, the main objective is to monitor the implementation of the Convention by a Party and to ensure that it complies with its commitments. When a Party encounters difficulties with the application of the Convention, the Convention Committee will provide assistance to the Party to comply with its commitments.

5. The pros and cons of adopting this regime

A State acceding to the Convention will benefit from a framed regime of transborder flow of personal data. As previously mentioned, for the adoption of an adequacy decision the European Commission will take account in particular the accession to the Council of Europe Convention 108 when assessing the level of protection in third countries or international organizations (recital 81a of EU General Data Protection Regulation).

Furthermore, State Parties will receive assistance and benefit from cooperation, in particular in the form of legislative expertise and help with bringing national legislation into line with international personal data protection standards.

Another positive aspect is that these States will enjoy the benefits of the Council of Europe's work and will take part in the work of the Consultative Committee. By acceding to the Convention, a state that is not a member of the Council of Europe may become a fully-fledged member of the committee and benefit from the forum it provides for sharing information. It is also possible that with the adoption of this regime, states could apply for observer status with the committee, without formally acceding.

In summary, this regime has multiple pros by being a global instrument safeguarding the right to privacy and a cooperation tool between parties.

However, it was argued that the Convention lacks a strong follow-up mechanism and that the consultative committee (T-PD) had limited resources and no real enforcement powers. Both hindrances will be addressed with the modernization of the Convention.

At a time when countries around the world are calling for a global instrument safeguarding the right to privacy, we do need to ensure that common core principles are in place in as many countries as possible to guarantee an appropriate level of protection of individuals with regard to processing personal data. Convention 108 can be the response to this call, and while governments can choose several paths to achieve the objective of global privacy standards, increased accession to Convention 108 is probably the easiest and most realistic one.

Data Protection in the East African Community

Robert Achieng, Senior Communications Engineer, EAC Secretariat

1. Background

Data protection and privacy laws are designed to regulate the collection, transmission, storage, use and access to personal data (i.e. data that identify, by whatever means, a natural person). The regulatory regime for data protection within the East African Community (EAC) is both comprehensive and evolving. It is comprehensive in the sense that it seeks to accommodate Partner States' duties and responsibilities with regard to, on the one hand, the safeguarding of human rights and fundamental freedoms, and on the other hand, the preservation of public security. Further, the regulatory regime evolves in tandem with advances in technology and the requirements for regional, continental and global harmonization.

In 2006, the EAC Council of Ministers directed that the EAC Framework for Cyberlaws ('Framework') be developed; a harmonized regulatory regime for data protection was to be an integral part of the Framework. The directive was inspired by the recognition of the growing societal influence of information and communications technology and the corresponding need to develop an appropriate policy and regulatory regime. Additionally, the directive drew its mandate from the EAC Treaty, notably Article 6 on Fundamental Principles (i.e. 'the recognition, promotion, and protection of human and people's rights') and Article 89 on Common Transport and Communications Policies (i.e. 'develop harmonized standards and regulatory laws, rules, procedures and practices').

The Content of the Framework: The Framework is divided into sections, with each section dealing with one of the five conventional areas of cyberlaws, namely: electronic transactions, electronic signatures and authentication, cybercrime, consumer protection, and data protection

Like the other sections of the Framework, the section on data protection contains, among others, the principles and best practices for data protection legislation. It also contained some thoughts and suggestions for an institutional framework.

The EAC Framework took an overtly cautious stance on data protection legislative reform. In

particular, the Framework refrained from discussing or recommending various legislative approaches (e.g. amending existing or enacting new statutes). Again, and unlike the approach adopted for the other sections, it did not provide a template for national data protection legislation nor a reference to a similar international instrument. Rather, it recommended that Partner States, collectively and individually, undertake further research on data protection legislative reform. It was envisaged that the research would enlighten policy makers on, inter alia, (i) the critical importance of data protection and privacy laws, notwithstanding the necessity and pressures for measures to preserve public security, (ii) the need to safeguard the privacy of citizens in cyberspace, (iii) the necessity for incorporating a corresponding law on access to official information and (iv) the need to consider international practice and experience.

2. Principles

The Framework suggests some principles to be adopted/incorporated into data protection legislation. Following the adoption of the Framework, four of the five EAC Partner States (i.e. Kenya, Rwanda, Tanzania and Uganda) have enacted cyberlaws on electronic transactions, cybercrime and consumer protection. Kenya and Uganda have also developed Bills on Data Protection and Privacy; the Bills have not been enacted into law, though. The Bills adopted the generic principles on data protection, namely:

- (i) Definitions (e.g. personal data, data controller, data processor)
- (ii) Conditions for collection, transmission, access, storage, and use of personal data (e.g. the principle of fair and lawful use, principle of proportionality, consent of data subject, accuracy, transparent processing, cross-border issues)
- (iii) Responsibilities of data controllers and data processors
- (iv) Rights of data subjects
- (v) Exceptions/Limitations
- (vi) Offences
- (vii) Institutional framework

Despite the recommendations of the Framework, no further research has been undertaken on the issue of data protection legislative reform, at least at the EAC level. It is not clear, either, if any of the Partner States has undertaken such research. For example, the Bills by the Republics of Kenya and Uganda do not seem to have adequately addressed some contentious issues on data protection legislation, notably the issues of storage and transfer of personal data across borders and the balance between data protection and privacy and preservation of public security.

The AU Convention on Cybercrime and Personal Data Protection was adopted in June 2014, after being developed for about three years. Needless to say, the EAC Framework, which was developed in 2008 and adopted in 2010, does not draw references from the AU Convention. The development of the Kenyan and Ugandan Bills also predated the AU Convention. However, one may arguably suggest that the EAC Framework, the Bills in Kenya and Uganda, and the AU Convention were inspired by extant international instruments on data protection, especially the widely known EU Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data.

Regardless of structure and content, there is one notable difference between the EAC Framework and the AU Convention: the AU Convention is a treaty which, upon entry into force, is legally binding upon the signatory State Parties. On its part, the EAC Framework is a non-binding document, merely containing guidelines and templates to assist national authorities in enacting harmonized national cyberlaws.

3. Implementation Challenges and impacts

The Framework was adopted for implementation in May 2010. To date, four Partner States have enacted legislation on electronic transactions, electronic signatures and authentication, cybercrime, and consumer protection. No Partner State has enacted legislation on data protection and privacy, though Kenya and Uganda have developed the requisite Bills. The delay in enacting legislation on data protection may be attributed to a number of challenges, as outlined below.

Data Protection and Privacy vs Cybersecurity: For many years, a fierce debate has been raging on the right balance to be struck between data protection and privacy vis-à-vis cybersecurity. Advocates for civil liberties argue that robust data protection and privacy

laws are needed to preserve human dignity and also safeguard fundamental freedoms, particularly the freedom of thought and the freedom of expression. On their part, governments, aware of the dangers of unfettered freedom in cyberspace, seek to limit the freedoms in order to preserve public security. This debate was anticipated by the EAC Framework, hence the recommendation that further research be undertaken on this area. The debate has, however, not been resolved, neither at the national level within EAC Partner States nor in the international arena. This lack of consensus has no doubt contributed to the delay in enacting data protection legislation in EAC Partner States.

Transposing the Framework into national laws: scarcity of resources: Transposing the Framework into draft legislation requires both human and financial resources. Within EAC Partner States, there are few officials who understand the technological as well as the legal aspects of data protection. Moreover, to be successful, any legislative initiative for data protection would inevitably involve awareness creation and stakeholder consultations, exercises that require financial resources. The scarcity of both human and financial resources contributed to the delay in enacting data protection laws.

New uncertainties due to advances in technology: Two developments in technology have brought further uncertainties in the regulatory landscape for data protection, namely cloud computing and data analytics. Even before the rapid uptake of cloud computing, the issue of cross-border storage and/or transfer of personal data was fairly contentious. With cloud computing, the physical location of data cannot be precisely determined, and it may change rather too often. Cloud computing also tends to unfairly tilt the balance of control towards the cloud provider, at the expense of customers.

Data analytics may affect the definition of personal data. Personal data are defined as data that may be used to identify a natural person, by whatever means. Data that would ordinarily not identify a natural person may do so after the application of data analytics. Undoubtedly, these new uncertainties have led policymakers in EAC Partner States to delay the enactment of data protection laws.

4. Impacts

Direct and anecdotal reports from private businesses indicate that the lack of consistent data protection

laws across the five EAC countries has had negative impacts on businesses. In 2014, a telecoms service provider indicated that the lack of such laws was hampering its plans to establish a multimedia content distribution service (i.e. Netflix). Again, a number of private businesses have established data centers across the region, hoping to commercialize their assets. Their business plans would benefit from data protection and privacy laws.

Civil authorities will certainly benefit from data protection laws. In 2012, the EAC conducted a study on e-immigration services. The study recommended that Partner States enact data protection laws to underpin the roll-out of e-immigration services. Partner States have projects that involve collection of personal data in digital format (e.g. civil registration projects in Tanzania and Uganda and the urban security project in Kenya). Civil liberty advocates have called on the governments to enact data protection laws.

5. Pros and Cons

Data protection and privacy laws are good, and governments should take deliberate steps to enact them. The EAC Framework underscored the importance of data protection laws, even if it did not make detailed discrete recommendations on them. And there is general consensus among policymakers in EAC Partner States that data protection legislation is a critical component of the regulatory framework of the information society.

However, data protection legislative reform faces some vexatious issues, which need to be addressed. These include the controversy on privacy vis-à-vis cybersecurity, the contention over the jurisdiction of

cross-border storage and/or transfer of personal data, and the challenges of cloud computing and big data analytics.

6. Harmonization of data protection laws in EAC countries

With regard to data protection, the EAC Framework for Cyberlaws did not provide discrete recommendations for the enactment of national legislation. Neither did it provide reference to an international instrument for best practice. Instead, it recommended that further research be conducted in this area.

In the absence of clear guidelines, it is expected that there will be considerable divergence in the data protection legislation of Partner States. Such divergence is already evident in the structure of the Kenyan and Ugandan Bills on data protection.

Fortunately, an opportunity to save the situation exists. Given that no EAC Partner State has enacted data protection law, it is prudent that they collaborate in developing a harmonized data protection law. In line with the recommendations of the Framework, the starting point for the collaboration effort would be to undertake research and consultations with a view to finding solutions to both the contentious as well as the emerging issues on data protection legislation. Further, EAC Partner States may benefit from the European experience where the EU Directive 95 on Personal Data Protection resulted in a complexity of national laws, thereby frustrating efforts on establishing a digital single market. Instead of eventual separate national laws, EAC Partner States may be well advised to enact a single EAC law on data protection, considering that data protection has several cross-border elements.

ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection

*Dr Isaias Barreto Da Rosa, Commissioner for Telecommunication and Information Technologies,
ECOWAS Commission*

1. Introduction and Context

Information and Communication Technologies (ICTs) are indispensable tools in achieving the ECOWAS Vision 2020 of an ECOWAS of People since ICT is a cross-cutting sector that has an effect on all economic and social sectors: education, health, trade, governance, and others. To have an effect, confidence and security are two of the main pillars where ICT needs to play a vital role as a tool for socioeconomic development for the region.

Today, the significant progress made in the field of ICT, including the use of the Internet in everyday life, poses problems regarding the life and work of the users. There is increasingly frequent recourse to the processing of personal data in various areas of economic and social activities. The use of ICT facilitates processing and data exchange whereby personal data can be collected, processed and used without the person's knowledge.

It is in this regard that on 16 February 2010, the ECOWAS Heads of State and Government adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS to complement the 1993 ECOWAS Treaty. This Act, like all the other Community Acts in ECOWAS, was adopted based on an inclusive consultative approach: an expert validation meeting with all the stakeholders, sectorial Ministers meeting, the opinion of the ECOWAS Parliament and adoption by the Council or the Heads of State and Government.

2. Purpose of this Supplementary Act on personal data

The scope of the Supplementary Act is very broad, since it encapsulates the processing of all personal data. It aims to ensure that every individual, whatever his nationality or residence, with respect to his rights and fundamental freedom, including their right to privacy with regard to automatic or manual processing personal data concerning any individual is covered. The Act also aims to be put into place in each ECOWAS Member State, appropriate measures for fighting against infringements of privacy that could be caused by the collection, processing, transmission, storage and use of personal data.

From a legal perspective, the use of a Supplementary Act is more binding than a Directive, since its content in all the provisions is mandatory for all Member States and it is also directly applicable from the date of its entry into force (Article 9/3 of the Supplementary Protocol A/SP.1/06/06).

3. Principles and Institutional framework guiding the processing of personal data

The Act defines new principles and rights that ensure transparency of processing operations on information. Under these principles, the Act stipulates that any personal data processing must have received the consent of the person concerned except as otherwise provided in the Act and that everyone has the right to know and challenge the information and arguments used in an automated or manual treatment when results are used to oppose the individual. The personal data must be kept confidential and protected, in particular where the processing involves the transmission of data over a network.

In order to ensure compliance with the principles and rights enshrined in the provisions of this Supplementary Act, it is necessary to create an independent administrative authority to ensure compliance with the principles and rights enshrined. Therefore, any country without such an administrative authority is encouraged to establish one (Article 14).

The Act has the advantage of harmonizing the legal framework in the ECOWAS space. It is important to emphasize that, prior to the adoption of this Act, few ECOWAS Member States had existing legislation on personal data protection. There was also no legislation at the continental level; the ECOWAS Supplementary Act has served as the basis for the elaboration of the African Union Convention on data protection.

4. Implementation of the Act and challenges

According to the ECOWAS Supplementary Protocol A/SP.1/06/06, a Supplementary Act is binding on Member States, therefore, they shall implement it. However, there were many challenges during the implementation of the Acts adopted at statutory level (Heads of State and Government and Council of Ministers) due to two key factors:

1. Capacity of the Member States to adapt the existing legislation to the Community Text or to elaborate the law in compliance with the regional Act
2. Some provisions of the Act are not properly reflected in national legislations or are completely ignored.

The lack of adequate skill usually leads to long delays in implementing the Community Acts, including the Act on Personal Data Protection. To provide appropriate capabilities to Member States in adapting or elaborating a national law, ECOWAS and its partner UNCTAD conducted capacity-building programs during the period of 2013 to 2015 to provide enough skills to many experts in the ECOWAS region. During that period, UNCTAD organized training courses for hundreds ECOWAS policy and law makers on the Legal Aspects of E-Commerce to raise awareness particularly to lawmakers and government officials on key aspects to be considered for the drafting of Electronic Commerce Laws, as well as on e-Commerce for Practitioners that aims to promote e-Commerce in ECOWAS region.

Five years after the adoption of the Act some Member States have yet to implement it in their national legislation.

On the compliance issue, more frequently, even though adopted at the regional level, some Member States are still reluctant to adopt some provisions of the Acts due to political, security or administrative considerations. In fact, the new Article 9, point 8 of the “Legal Regime of the Community” of the Supplementary Protocol A/SP.1/06/06 Amending the Revised 1993 ECOWAS Treaty states Community Acts under consideration shall be adopted by unanimity, consensus or by two-thirds majority of the Member States. This means that even though adopted, some Member States may not be in favour of some provisions.

One of the key provisions in the Act is Article 14 on the establishment of an independent Data Protection Authority in each Member State. To date, few Member States have complied with this provision.

5. Importance of harmonization

Harmonization is a prerequisite for the establishment of a common liberalized ICT market and trade facilitation, including electronic transactions that affect the issue of personal data. Indeed, e-commerce and information exchange should be subject to the same rules within the ECOWAS community to ensure better protection for consumers beyond the borders of a Member State. The same challenge can be faced by businesses that have cross border activities.

Data protection in the European Union: Today and Tomorrow

Lukasz Rozanski, Policy Officer, Data Protection, European Commission

1. Context

Data protection is recognized as a fundamental right under the EU Charter of Fundamental Rights, as well as under the Treaty on the Functioning of the European Union (TFEU). Article 8 of the Charter establishes the right to data protection, while Article 16 of TFEU specifically covers the Union's ability to legislate on data protection.

The most important current provisions for EU data protection are contained in Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC or the Directive). A directive is an instrument addressed to Member States that must be implemented in national legislation. Some sector-specific provisions also exist (e.g. Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector).

2. Main principles and enforcement

Under the Directive, information is considered to be 'personal data' if it relates to an identified or identifiable natural person. The Directive applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non-automated filing systems (traditional paper files). It does not apply to the processing of data by a natural person in the course of purely personal or household activities. Furthermore, processing in the course of an activity falling outside the scope of EU law, such as operations concerning public security, defence or State security, are excluded from the scope of the Directive. Personal data processed by public authorities for the purpose of preventing, investigating, detecting or prosecuting a criminal offence, or of executing a criminal penalty, are subject to the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Under the Directive, the processing of personal data is lawful only if:

- the data subject has unambiguously given his consent;
- processing is necessary for the performance of a contract to which the data subject is party;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or
- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

The Directive also contains a number of principles that must be observed whenever data are processed. Personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive, accurate and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected.

In principle, processing personal data falling within special categories is forbidden, namely those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Such processing is allowed in exceptional cases, notably in case of explicit consent of the data subject, the need to protect vital interests of the data subject or the need to protect legitimate interests of others. Member States may also, on an exceptional basis, allow for the processing of such data for reasons of substantial public interest.

Each person whose data are processed (data subject) can exercise the following rights:

- the right to obtain information: the controller must provide the data subject from whom data are collected with certain information (the identity

of the controller, the purposes of the processing, and recipients of the data);

- the right of access to data: every data subject should have the right to obtain confirmation of processing from the controller, “without constraint at reasonable intervals and without excessive delay or expense”;
- the right to rectification, erasure or blocking of data processed in a non-compliant manner; and
- the right to object to the processing of data: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him. (S)he should always have the right to object to the processing of personal data for the purposes of direct marketing.

However, the scope of certain obligations and rights mentioned above may be restricted if necessary to safeguard—among others—national security, defence, public security, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union, or the protection of either the data subject or the rights and freedom of others.

The Directive requires the Member States of the EU to establish and ensure the functioning of independent supervisory authorities responsible for monitoring and enforcing the application of the national provisions that implement the Directive, within their respective territories. Processing operations have, in principle, to be identified to the competent national supervisory authority before they can be carried out.

Every person enjoys the right to an administrative and judicial remedy for any breach of rights guaranteed by national law applicable to the data processing in question. A person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for such damage.

A Working Party on the Protection of Individuals with regard to the Processing of Personal Data has been set up, composed of representatives of the national supervisory authorities, representatives of the European Data Protection Supervisor, and a representative of the Commission. It is charged with the task of examining any question with regard to the application of the national rules adopted in implementation of the Directive, advising the Commission (including through opinions on the level of data protection in

third countries) and making recommendations on all matters relating to data protection.

3. The way forward

EU legislation on data protection has been in place since 1995. Although Directive 95/46/EC guarantees an effective protection of the fundamental right to data protection, differences in the way that Member States implement the Directive have led to complexity and, sometimes, legal uncertainty. The current rules also need to be updated in the light of technological developments and new threats to the fundamental right to data protection.

For this reason, a comprehensive data protection reform was proposed by the European Commission and agreed upon, in December 2015, by the EU legislative bodies, the European Parliament and Council of the EU. The new rules are expected to be formally adopted in the first semester of 2016 and will become applicable two years thereafter.

As part of the reform, Directive 95/46/EC will be replaced by a General Data Protection Regulation (GDPR) that sets out a general EU framework for data protection. The system will be complemented by a directive about the processing of data by competent authorities for the purposes of the prevention, detection, investigation or prosecution of criminal offences and related judicial activities (Police Directive).

The GDPR updates the data protection principles enshrined in Directive 95/46/EC. It is based on three main building blocks.

First, the GDPR provides for a uniform and simplified legislative framework. It will establish one single pan-European set of rules that will make it simpler and cheaper for companies to do business in the EU, and will ensure that the rights of individuals are more effectively protected across the continent. Consistency of interpretation of the new rules will be guaranteed. In particular, in cross-border cases where several national data protection authorities are involved, a single supervisory decision will be adopted. This “one-stop-shop” mechanism means that companies will not only deal with one law, but also with one single supervisory authority (instead of 28). The same data protection rules will apply to all companies offering goods or services on the EU market, regardless of where they are established. This will ensure fair competition by creating a level playing field for all market players. The new rules will also abolish most requirements on notification and pre-authorization of

processing operations, thereby significantly cutting red-tape.

Second, the reform seeks to empower individuals with more control over their personal data. This is done by updating and adapting individuals' rights, and the corresponding obligations of controllers and processors, to the challenges and opportunities of the digital age. This includes the introduction of new tools such as the right to data portability that will make it easier for individuals to transmit personal data between service providers, or the notification of data breaches that put individuals at risk, so that supervisory authorities and/or users can take appropriate measures as quickly as possible. Data protection "by design" and "by default" will ensure that safeguards will be built into products and services from the earliest stage of development and that privacy-friendly settings will be the norm – for example on social networks or mobile apps. According to the risk-based approach, certain core obligations will be tailored to the specific risks of the processing operation in question, thereby avoiding a burdensome one-size-fits-all approach.

Third, the GDPR provides for stronger enforcement of the rules. Cooperation between national data protection authorities will be strengthened, including joint investigations. Credible and dissuasive sanctions are provided in case of any violation of the rules. Companies may face fines of up to four percent of their global annual turnover.

In sum, the data protection reform will strengthen the fundamental right to data protection by allowing people to regain control over their personal information. This will increase their trust when giving or allowing the collection of their personal data, in particular in the on-line environment, and can thus contribute to the further development of the digital economy. As a contemporary, homogenous and comprehensive framework for data protection rules covering a large economic area and important trading power like the European Union, the GDPR will also be an important contribution to the development of global data protection standards.

4. International aspects

Both current and future data protection rules authorize transfers of personal data from a Member State to a third country only under certain, restrictive conditions. This is specifically the case when the Commission determines that the non-EU country provides an adequate level of protection (so far 11 countries have been deemed "adequate", including Canada, New Zealand, Switzerland and Uruguay). When an adequate level of protection is not guaranteed, the Directive provides for a number of alternative grounds on which transfers may nevertheless take place. Transfers may be carried out where adequate safeguards are adduced, e.g. by means of standard contractual clauses or binding corporate rules (applied within a group of companies). Furthermore, transfers may take place under a number of derogations, notably where the data subject agrees to the transfer, where the transfer is necessary to perform a contract or where the transfer is necessary on public interest grounds.

This system is generally maintained, but streamlined in the GDPR. New instruments of transfer have been added to facilitate the international exchange of data (e.g. approved codes of conduct and approved certification mechanisms).

The EU is actively involved in international cooperation on data protection through various international fora, including the OECD and the Council of Europe (and it intends to become a Party to the Council of Europe's revised Data Protection Convention 108). The EU participates in the dialogue on privacy and data protection with regional organizations, notably with APEC. This dialogue aims at achieving a better understanding of the respective data protection systems of various jurisdictions, in order to address potential obstacles to the international exchange of data more fully. Foremost is the need to ensure continuity of protection when the personal data of Europeans are transferred outside the EU.

Private Sector and NGOs



Personal Data Protection and international data flows: the case of Brazil

Rafael Zanatta, *IDEC (Brazilian Institute of Consumer Defense)*

1. Introduction

Despite being a progressive nation in the use of the Internet, with more than 100 million Internet users,¹⁰⁷ and a globally known advocate for civil rights on the Internet,¹⁰⁸ Brazil has an incomplete regulatory structure for consumer protection, e-commerce regulation, and data protection. This situation presents challenges for international cooperation, the growth of the digital economy and the protection of collective rights. This article explains how the regulatory mechanisms for data protection function in Brazil and the content of a draft law for personal data protection first proposed six years ago.

2. Why is Brazil different? Data protection in historical perspective

During the late 1980s, Brazil went through a process of institutional building after the civil-military dictatorship (1964-1985). The Constitution of 1988 provided legal grounds for the protection of intimacy (Article 5, X), the rights to access and correct information in the possession of a data controller (Article 5, XIV), and a right to a judicial hearing about personal data using the remedy of *habeas data* (Article 5, LXXII).

2.1 The relationship between consumer protection and data protection

The major legal innovation for protection of personal data occurred during the 1990s. Social movements and organizations for collective rights, like IDEC, helped the government to enact the Consumer Protection Code (Law 8078/90), a federal law that “sets forth the standards for consumer protection and regarding public policy and social interests, pursuant to arts. 5, XXXII, 170, V, of the Federal Constitution” (Article 1). In this Code, a section on “Consumer Databases and Registries”. Article 43 reads as follows:

Art. 43. The consumer, without prejudice to the provisions in art. 86, shall have access to existing information in registries, forms, records and personal data and consumer files about them, as well as their respective sources.

1§ The records and consumer data shall be objective, clear, truthful and in a language that is easy to understand and cannot contain negative

information concerning a period about five years.
2§ The opening of a consumption registry, form, record and personal data must be communicated in writing to the consumer, when not requested by the consumer.

The Code also created mechanisms for administrative sanctions for violation of consumer protection rules (Article 55) and established the “National Consumer System” (Article 105), coordinated by the National Bureau of Consumer Protection, an organ that operates inside the Ministry of Justice (Article 106).

In a sense, consumer protection agencies also had the responsibility of dealing with personal data protection. The downside was the lack of a general law about personal data protection, following the trend established by European countries (Directive 95/46/EC of the European Parliament and Council).

2.2 Marco Civil da Internet and the lack of a general personal data protection law

In 2007, the idea of a “civil framework” for the use of the Internet was proposed by Ronaldo Lemos and researchers of the *Centro de Tecnologia e Sociedade* (FGV Law School). This proposal was adopted by NGOs and activists that pushed the government to create new rules on net neutrality, freedom of expression and privacy. This network of digital rights activists penetrated the Ministry of Justice and, in 2009, the federal government launched a public consultation for a new law called “Marco Civil da Internet”.¹⁰⁹

On April 2014, Marco Civil da Internet (Law 12.965/14) was enacted. The law declares in Article 3 that the discipline of Internet use in Brazil has the following principles: guarantee of freedom of speech and expression of thought; protection of privacy; protection of personal data, pursuant to law; preservation and guarantee of network neutrality; preservation of functionality of the network; liability of agents according to their activities; preservation of the participative nature of the network; and freedom of business models promoted on the Internet.

It is important to notice that the protection of personal data is limited in this law. The legislature declared that

there must be a separate law to deal specifically with data protection. However, Marco Civil established new rights and principles regarding privacy, data protection and data retention. They can be summarized as follows:

- Inviolability of intimacy and private life, safeguarding the right of protection and compensation for material or moral damages resulting from their breach (Article 7, I);
- Inviolability and secrecy of user's stored private communications, except upon a court order (Article 7, II);
- Non-disclosure to third parties of user's personal data, including connection records and records of access to Internet applications, unless with express, free and informed consent (Article 7, VII);
- Clear and complete information on the collection, use, storage, processing and protection of user's personal data, which may be used for the purposes that justify their collection and are specified in the agreements of services or in the terms of use of the Internet application (Article 7, VIII);
- The need for a specified and separate contractual clause to obtain the expressed consent for the collection, use, storage and processing of personal data (Article 7, IX);
- The definite elimination of the personal data provided to a certain Internet application, at the request of the users, at the end of the relationship between the parties (Article 7, X);
- The compliance of personal data, connection logs and the content of private communications with the protection of privacy (Article 10); and
- The obligations of foreign companies (Internet providers and applications providers) to comply with the Brazilian personal data rules if they do any operation of collection, storage, retention and treatment of personal data in the national territory (Article 11).

3. Regulatory mechanisms and the proposal of a new law

3.1 The data protection obligations proposed by the government

Since 2010, the Ministry of Justice has been attempting to enact a draft bill on personal data protection.¹¹⁰ This process, however, is being highly disputed by the private sector, which claims that self-regulatory mechanisms (codes of conduct developed by the

private firms) are a better regulatory strategy, rather than creating a new institutional structure (a federal agency for personal protection) for this issue.¹¹¹

The draft bill applies to individuals and companies that process personal data via automated means, if the personal data were collected in Brazil.¹¹² As proposed by the Ministry of Justice, the bill would impose new obligations on the private sector. According to the analysis made by the *Privacy & Information Security Law Blog*, the new draft bill:¹¹³

- Creates a requirement to obtain free, express, specific and informed consent to process personal data with limited exceptions (if the law demands the collection/treatment and if pre-contractual procedures are already accepted by the party);
- Prohibits the processing of sensitive personal data, with limited exceptions;
- Creates the obligation to immediately report data breaches to the competent authority;
- Allows data subjects to access their personal data and correct if incomplete, inaccurate or out-of-date;
- Creates restrictions for transferring personal data to countries that do not provide similar levels of data protection;
- Sets up obligations to adopt information security measures that are proportional to the personal data processed and to protect the information from unauthorized access, destruction, loss, alteration, communication or dissemination.

The current draft bill also has many innovations compared to the 2010 version.¹¹⁴ The concept of personal data does not include identification of equipment but involves all the forms of data that relate to an identified or identifiable person (Article 5, I). The data collection and data processing must be aligned with "legitimate expectations" of the subject (Article 6). There is the possibility of "granular consent", that is, individuals can provide fragmented authorizations moving beyond an "all or nothing" standard (Article 9, § 4º). Anonymized data can be considered personal data if the "anonymization process" (technique to make the personal data anonymous) can be reverted (Article 13). The bill also creates the "data portability right" (Article 18, V), emulating the European proposal to create "a right that would enable data subjects to transfer their personal data in a commonly-used

electronic format from one data controller to another without hindrance from the original controller”.¹¹⁵

Finally, the draft bill on personal data protection also creates obligations for the public sector (Articles 23 to 30) and has one special chapter on international data transfer. According to the governmental proposal, the new law would read as follows:

Art. 33. The international transfer of personal data is allowed only in the following cases: I – for countries that have an equal level of personal data protection; II – when the transfer is necessary for international legal cooperation between public organs of intelligence and investigation, in accordance with instruments of international law; III – when the transfer is necessary for the protection of life or physical integrity of the subject or third party; IV – when the competent authority allows the transfer; V – when the transfer results in a compromise assumed through an international cooperation agreement; VI – when the transfer is necessary for the execution of a public policy, according to article 24; VII – when the subject has given his consent for the transfer, with previous information about the international character of the operation, being informed about the risks involved.

In the new proposal, Brazil must establish a new public authority for the definition of the conditions of data transferability. However, the proposal is too abstract and does not specify the composition of the “competent organ”. The bill is also confusing, because it creates two new institutions, the “new authority/organ” and the “National Council of Personal Data Protection and Privacy,” that have related functions.

3.2 What is happening without the new general data protection law?

The ideal scenario is still distant. There are many reactions against this draft bill, especially from the advertisement industry.¹¹⁶ For many representatives of the private sector, the existing rules (Code of Consumer Protection and “Marco Civil da Internet”) are enough for the protection of personal data in Brazil – a vision that is highly contested by NGOs and digital

rights activists.¹¹⁷ This tension makes things difficult for the Ministry of Justice and the executive power.

Without a general law for personal data protection and one federal agency to execute these norms and monitor the private sector, the strategy adopted by the government was to reinforce the mechanisms of protection collectively inside the Ministry of Justice. This happened in 2014, when the National Bureau fined the private company Oi 3.5 million Brazilian reais (1 million US\$) for monitoring the data of all its home broadband Internet customers. This example might show that the data protection regime in Brazil is working even without a federal agency for this area.¹¹⁸ However, this reasoning is misleading. The problem is that the National Bureau does not have an institutional structure to deal with cases of data protection, which are highly complex and involve technical expertise. The Department of Protection and of Consumers must deal with all the cases of violation of collective rights, including difficult cases concerning health insurance and telecommunication. In other words, this structure is not capable of providing a reasonable level of protection because there is too much work to do, in all areas of consumer rights.

4. Conclusion

It is clear that the field of digital rights has advanced in Brazil. The enactment of the Marco Civil da Internet (Law 12.965/14) and new e-commerce law (Decree 7.962/13) expanded the protections already set forth in the Code of Consumer Protection. However, the government was unable to enact a new general law on data protection law. Consequently, the country still lacks an independent regulatory authority for this issue and does not have specific rules for the private sector, like the obligation to appoint a data protection officer and develop policies for privacy protection.

International data flows are allowed as long as they comply with Law 12.965/14. However, Brazil needs more norms and institutional structures. In a world of increased complexity and with the rise of specialized global policy communities, Brazil is missing an opportunity to create one agency dedicated to this issue and collaborate in a global level for better regulations, compliance and protection of collective rights.

Cross-border e-commerce: building consumer trust in international data flows

Liz Coll, Consumers International

1. The rise of e-commerce

The Internet has brought about a revolution in the way goods are bought and sold. Since the first secure transactions in the mid-1990s, there has been a rapid growth in business-to-consumer e-commerce. Data for 2014 estimated it to be worth \$1.5 trillion worldwide (up 42% percent since 2012¹¹⁹) and it is predicted to reach \$2.36 trillion by 2017. Growth in more recent years has been in part generated by the rapidly expanding online and mobile user bases in emerging markets¹²⁰. An estimated \$1.2m is spent online every 30 seconds¹²¹, with a fifth of that going through the world's biggest e-tailer, Alibaba.

Despite the internet granting consumers unprecedented direct access to international markets, cross-border e-commerce has grown at a much slower rate than its domestic counterpart. Only around a quarter of consumers engaged in e-commerce made an international purchase in 2015¹²². This disparity will partly reflect the extent to which domestic markets meet national demand - thus limiting the scope for cross-border sales, but it will also relate to issues around consumer trust and confidence. Data for member states in the European Union show that consumers are considerably more confident buying online domestically (61 percent are confident) than from other member states (38 percent)¹²³.

Barriers to trust and confidence that arise in relation to domestic e-commerce (including delivery delays, hidden costs and fear of fraud) can be exacerbated when it comes to cross-border transactions. Other barriers will be distinctly cross-border in their nature and relate to:

- Confidence in dealing with unfamiliar brands in a different language;
- Hidden costs linked to customs duties and currency conversion, as well as costs that arise from distance (such as shipping or delivery);
- Availability of preferred payment methods;
- Conformity of products to local standards; and
- Lack of clarity on protections afforded by the vendor's jurisdiction; and what recourse and redress is available if things go wrong.

2. Understanding the data dimension

Data are as critical to facilitating an online transaction as making a payment; indeed in some cases data replace financial payment (for example social media platforms). Sensitive information such as delivery address and payment details is actively provided by consumers, but the extent to which wider data are gathered by the vendor is often unclear. Search habits, purchase history, location and ISP address are collected in ways that can be difficult for consumers to understand or prevent. When this is aggregated with other data, companies and third parties can develop an in-depth picture of people's preferences and likely purchasing intentions.

Research shows that concerns about personal data use and/or misuse are a central driver of trust in online markets and can compound the barriers highlighted above. Of course, personal data gathering is not limited to e-commerce; it is part of a much bigger digital experience of constant data collection. Through social media, personalized apps, wearable technology, sharing platforms, search and targeted products, people are continually exposed to the effects of data collection, aggregation and onward sharing. Concern about these effects varies between different countries but is consistently high, and rising – with an annual tracker of consumer online attitudes putting US consumer worries about online privacy up 42 percent¹²⁴ and UK concerns up by a third since 2014¹²⁵.

A 2014 global survey of 16,000 online consumers across 20 countries¹²⁶ found that 74 percent were concerned about how companies use information about them collected online. Worldwide, 72 percent of respondents did not know what information is known about them by companies and 63 percent did not know what rights they have over companies handling their information. In terms of financial information, in Europe 55 percent fear becoming a victim of fraud via online transactions¹²⁷ and 58 percent abandon a purchase because of fears over payment security.¹²⁸ These fears appear well founded, with a 2015 report claiming data breaches globally were up by 40 percent on the previous year.¹²⁹

These levels of concern are in part due to consumers' sense that they have lost control over how data are

collected and how companies utilize it once in their possession. Terms of use that purportedly detail company practices are opaque, long and complex¹³⁰ –they are geared towards organizational compliance and liability limitation, not consumer comprehension.¹³¹ Consumers are faced with a ‘take or leave it’ choice when considering whether to use or not use an online service, with limited opportunities to assert their own preferences. While it may be in the interests of many companies to interpret ongoing participation within the current set up as satisfaction or acceptance, research suggests a consumer resignation to having lost control,¹³² which adds to the loss of trust. Global research reflects a similar sense, with 72 percent agreeing that it was inevitable that privacy will be lost because of new technology.¹³³

“[there is]... a decline in trust among all stakeholders. Individuals are beginning to lose trust in how organizations and governments are using data about them, organizations are losing trust in their ability to secure data and leverage it to create value”¹³⁴

This decline in trust, recognized by consumer advocates and businesses alike, is what national and international regulators must now contend with.

3. Regulating the digital age

The creation of effective regulation and policy to enable more trust in the digital economy is a pressing challenge. Networked platforms such as Facebook, Uber or AirBnB have shown how online services can achieve huge scale in a short space of time – showing how innovation can now outpace institutions responsible for consumer protection. What is more, these disruptive services have a transnational reach, hence requiring a response that is coordinated at the international level – something that adds further lag. Members of Consumers International have voiced their concern, with 80 percent feeling legislation, regulation and standards relating to redress are ineffective at keeping pace with the digital economy, and 76 percent doubting the efficacy of enforcement.

Take data protection law: prior to the recent spate of revisions, consumer privacy and data protection had not been considered by Europe, the UN or the OECD since the last century. Currently in the European Union, member states are working to overhaul rules adopted before Google.com was even registered as a domain name. In the intervening period, an unprecedented shift has taken place: not just in the amount of data collected at an individual level, but in the ways in which

it is used by companies and public organizations to identify large scale patterns in consumer and citizen behaviour, or to identify and tailor information, or to target individuals.

Consumers International has been an active participant in seeking to update some of the international instruments for this new world. The revised Guidelines on Consumer Protection from the United Nations (UNGCP) establish both a new ‘legitimate need’ for the protection of consumer privacy and the global free flow of information, and a new chapter containing principles for good practice that seek to require business to protect privacy through consumer control, security, transparency and consent mechanisms. But in the context of the perpetual changes and challenges wrought by technology, consumer protection mechanisms need to be not just principled, but responsive and adaptable across borders. It remains to be seen whether welcome advances such as the UNCGP or EU General Data Protection Regulation will be able to respond effectively if the pace of change over the next 20 years corresponds with that of the last two decades.

Given the limitations that are becoming apparent in conventional institutional approaches, it may be that new innovation will provide solutions to some of the challenges that prior innovation has created. E-commerce has a history of developing such innovative solutions, and the emergence of new personal data empowerment tools and services that return some agency over data to consumers suggests a response to data concerns that could build on regulation and legislation.

4. Consumer involvement in regulating e-commerce

The ability to build trust, assure security and provide positive user experiences has long been a prerequisite for operating successfully across the web and across borders. As new, virtual marketplaces were created, they threw up numerous challenges which the old twentieth century regulatory rules book could not adequately cover. Rather than wait for new regulations to be drafted, players responded with practical, innovative mechanisms to address concerns and inhibitors to engagement. These mechanisms have often involved and relied on consumers much more than traditional regulation, and they continue to be iterated today to reflect developments and regional differences. Despite the fact that the majority of consumers will only choose to have a minimal

involvement, a level of trust and confidence is maintained since the system has consumer opinions and preferences built in.

- **Verification:** AirBnB – when operating as a small platform, a formally verified identity for a guest or host was not available – payment and reviews sufficed. With expansion, more sophisticated mechanisms were required, which blend official documentation and links to social profiles, to complement the host and guest reviews on the site.¹³⁵
- **Dispute resolution:** Online dispute resolution (ODR) platforms have emerged to make it much simpler for a merchant and a dissatisfied consumer to reach a resolution. Modria, a leading provider of ODR services, handles more than 60 million disputes per year - a case volume many times larger than the US court system.¹³⁶ Research shows that making use of the ODR process increased usage of the marketplace, regardless of outcome.¹³⁷
- **Reputation and ratings:** eBay addressed the problem of buying from strangers with its reputation and rating system, enabling consumers to judge the trustworthiness of a vendor, and have visible recourse in the event of problems arising.
- **Payment:** In China, 60 percent of online purchasers utilize Alipay – an escrow payment system where consumers' payments to a third party are only released to the vendor once the goods have been received and declared satisfactory.

These have not done away with the need for legislation or formalizing particular rights and responsibilities, but they have helped to enable trade between participants and given some confidence to consumers. Besides just processing a financial transaction, they provide for the construction of trust between participants.¹³⁸

5. Implications for the data dimension: can technology respond to the challenges that technology creates?

Given the propensity of innovation to develop tools that enable consumers to play a role in managing concerns related to trust and confidence in other areas of e-commerce, what is the potential for it to deliver greater confidence in data use? As well as knowing precisely what makes consumers so uneasy about

current data flows in e-commerce, there is clarity on the things that would reassure them. Research consistently finds that consumers would like more control, access, transparency and accountability from providers about how their data are collected and used.

Traditional protection remedies concentrate on controlling how businesses collect, store and use personal data, and is reliant on regulators and business to make the system work, which leaves the consumer as a passive 'data subject' in the system with little room for manoeuvre. Yet this classic conception of legislation and regulation may not be able to provide full reassurance. In the European Union, for example, with one of the strictest data protection regimes in the world, confidence in data handling remains low.¹³⁹

However, the prospect of low cost, personalized technology to deliver consumers' individual privacy and data sharing preferences is resulting in the emergence of a number of new tools and services that help individuals assert more control over how their data are collected and used, by whom and for what purposes.¹⁴⁰ These emerging personal data empowerment tools put the individual consumer preferences back into the equation in a way that traditional regulation does not, and move beyond informed consent tick boxes and onerous terms and conditions. For example, apps on a smartphone can alert users when their data are being accessed outside of a person's set preferences, or tools that give a behind the scenes view of what data are being collected by whom. Such services effectively take on the role of data intermediary between suppliers and customers, working on behalf of the consumer to ensure their sharing and usage preferences are met.

Examples of personal data empowerment tools and systems

- **Personal data stores:** secure storage of data, which are authorized to transact and share data with chosen businesses or state services according to terms set by consumers. Stores would also audit use and alert or fix when criteria are not met..
- **Person-centred permissions:** dashboards where consumers can set and change data sharing privileges, invoke time stamped permissions which expire when consumers chose, and view which data are going where.¹⁴¹
- **Trust networks:** simplifying sharing choices through the creation of a network of accredited, trusted providers who commit to using consumer data on individual consumers' terms.¹⁴²

Personal data empowerment tools and services demonstrate an additional new way of responding to risks and concerns about data and privacy— one that can build on regulation, whilst not negating the need for it. This is a nascent market, but one that could potentially achieve higher levels of trust and confidence by involving consumers and empowering them to regulate the way companies use their personal data. However, in much the same way that shared information obligations or common returns policies help underpin confidence in cross-border e-commerce, there is a role for coordinated international regulatory systems to support their development and enable them to flourish in the following areas:

- **Upholding protections and rights:** agreed and enforced protocols on data breach notifications and remedies would give consumers more clarity on how their rights would be upheld. Dispute resolution protocols that can operate at a global scale could be developed and used if/when problems arose.
- **Establishing minimum standards:** agreed standards on privacy by design could see a higher level of privacy as a default setting of services. Encryption requirements could be used to increase security of data.
- **Incentivising good practice:** operators of personal data stores or trust frameworks would be held to high standards of transparency and

audit, with easily recognizable credentials to help consumers choose between providers.

- **Creating a competitive market** for services that offer consumers a way to easily control and manage their privacy and sharing preferences. Crucial to this will be establishing rights to data portability and agreed specifications on interoperability between platforms, so that individual privacy and sharing preferences could be aggregated around a person and easily transported between services. This has the potential to give consumers a share in the utility value of their data and increase their leverage in the marketplace.

In conclusion, a number of factors deter consumers from participating in cross-border trade, not least of which are the concerns that consumers have with online data use in wider digital interactions. For e-commerce to grow within and between countries, regulators must think not just about aligning regimes and rules across borders, but about how to create the space for the sorts of innovative approaches described above to build trust in data use. User-friendly mechanisms that enable control and choice over who sees or stores their data and who it is shared with, and transparency and understanding about what it is used for (backed up by internationally agreed requirements) will be part of the solution to creating a trusted environment in which consumers can make the most of the opportunity of global e-commerce.

Comments of the Computer & Communications Industry Association on Data Protection Regulations and International Data Flows: Impact on Enterprises and Consumers

Bijan Madhani, Public Policy & Regulatory Counsel and *Jordan Harriman*, Policy Fellow, CCIA¹⁴³

The Computer & Communications Industry Association (CCIA) submits these comments for consideration by the United Nations Conference on Trade and Development (UNCTAD) for its study on data protection regimes and international data flows. CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. Robust international data flows and interoperable privacy regimes are crucial to the success of CCIA members, as well as other industry sectors that depend on our members' services. CCIA members employ more than 750,000 workers and generate annual revenues in excess of \$540 billion.¹⁴⁴

1. Importance of Cross-Border Data Flows

International data flows have transformed modern trade in goods and services. Data flows create new pathways for commerce and investment, and also allow companies to operate more efficiently. Cross-border e-commerce in goods and services continues to grow in absolute value and as a share of overall trade.¹⁴⁵ Internet platforms allow small- and medium-sized enterprises (SMEs) around the world, especially in developing countries, to reach more customers online with decreasing marginal costs.¹⁴⁶ And as goods production becomes more fragmented and dispersed into global value chains, data flows have also become essential to non-services fields like manufacturing.¹⁴⁷

With the growth of digital flows and e-commerce have come concerns about the protection of personal data, and the security of digital transactions and content. These concerns are not just shared by consumers. Protection of data is at the core of the Internet's sustained growth as a platform for expression and trade in goods and services. In fact, the lifeblood of Internet-based industry—which today has grown to include a substantial component of all industries—is the trust that global Internet users have in online platforms.

Though data flows across borders with greater speed and quantity than ever before, laws and regulations on data protection are generally set on a national

or regional basis. At times, this can create conflicts between data protection laws due to differing priorities with respect to consumer protection, law enforcement access, and national security exemptions. To ensure that data flows are not unnecessarily impeded, it is essential that countries develop interoperable data privacy regimes that allow data to move freely, while also providing substantial protections for data belonging to consumers and businesses.

Interoperable regimes are important for a variety of reasons. They provide baseline legal certainty that data flows will not be unduly restricted, which gives businesses the confidence to operate and invest freely. This is key for creating an environment for SMEs to participate in cross-border data flows. Such regimes also increase confidence for customers by setting international standards for data privacy and assuring equitable protection for users' data regardless of their country of citizenship.

Interoperable regimes also contribute to the reduction of cost and process burdens on companies conducting international business. Data transfers are not just essential for completing an online transaction, they are critical to the production process for a range of goods and services. And very often, personal data—like subscriber data, employee information, and business contacts—are involved heavily in these production-process transfers.¹⁴⁸ Increased compatibility and flexibility between varying systems can lead to lower barriers to entry for SMEs entering and operating in new or developing markets.

2. Case Study: U.S.-EU Safe Harbor Framework

The long-standing U.S.-EU Safe Harbor Framework, in light of its recent invalidation by the Court of Justice of the European Union (CJEU), is instructive as to the high stakes of global e-commerce and the value of maintaining interoperable data protection regimes.

The transatlantic relationship between the United States and European Union is a significant component of both economies, as each is the other's largest market for goods and services.¹⁴⁹ Within that vital relationship, digital trade continues to increase in

relative importance as digitally delivered services become more and more essential to overall economic activity. In 2012, the Brookings Institute estimated that U.S. exports of digitally deliverable services to the EU were worth \$140.6 billion, or 72% of services exports, and the EU's share of digitally deliverable exports to the U.S. comprised 60% of services exports, amounting to \$106.7 billion.¹⁵⁰

Until its invalidation, the Safe Harbor Framework had been used by more than 4,000 U.S. companies, along with the U.S. subsidiaries of EU companies, to lawfully transfer data about EU citizens from Europe to the United States in compliance with European data protection regulations.¹⁵¹ In addition to being a direct contributor to the economic benefits that inure from transatlantic digital trade, the Safe Harbor was a boon to transatlantic digital innovation. The efficiency gains from unimpeded cross-border data flows enabled small businesses on both sides of the Atlantic to enter previously inaccessible markets and compete at scale. In fact, a full sixty percent of the companies who had certified compliance with the requirements of the Safe Harbor Framework were small- and medium-sized enterprises.¹⁵²

In October of 2015, the CJEU ruled against the legal underpinnings of the EU-U.S. Safe Harbor Framework. This ruling has had considerable impacts on transatlantic data flows. Thousands of businesses—small and large—that previously transferred personal data from Europe in compliance with the Safe Harbor Framework have had to find alternative mechanisms to ensure that they can continue to do so in compliance with EU law.

The currently available alternatives to permit EU-compliant data transfers are complex legal mechanisms, including binding corporate rules and standard contract clauses.¹⁵³ Both options are costly, piecemeal, time-consuming, and difficult to implement for even the most sophisticated companies. Expecting small- and medium-sized enterprises to successfully adopt these alternatives, particularly in the short term, to comply with the varying requirements of the data protection authorities of each EU member state would seem unlikely. These other transfer mechanisms are also at risk of being invalidated.¹⁵⁴

In the long term, the absence of a clear, reliable mechanism for lawful transfer of data across the Atlantic would lead to significant economic consequences. Larger companies could attempt to

comply with the implications of the ruling by building costly local facilities for processing and storage of data in the EU. Smaller firms will likely not be able to bear this burden, and could be forced to exit European markets. In 2013 it was estimated that a serious disruption of this very kind to cross-border data flows with the EU would likely cost the EU between 0.8% and 1.3% of its GDP.¹⁵⁵

Fortunately, a revised agreement between the U.S. and the EU was recently agreed upon. The new EU-U.S. Privacy Shield attempts to strike a delicate balance between the ongoing need for data-driven innovation to benefit consumers and small businesses and to drive economic growth, and a responsible, principles-based framework to ensure consumer protection. The EU-U.S. Privacy Shield is an effort to bridge different legal frameworks for data protection and may be an inspiration for other systems designed to ensure interoperability between other countries and for other types of data.

3. Costs of Restrictive Data Protection and Localization Regimes

As the invalidation of the Safe Harbor Framework demonstrates, the potential costs to businesses of complying with a number of different data protection regimes can be significant in the aggregate. A recent OECD report highlighted studies which indicate that compliance costs for SMEs not in the ICT sector can increase those companies' IT expenditures by as much as 40%.¹⁵⁶ The report also highlighted another survey, focused on multinational corporations, which found data-related compliance costs averaged over \$1 million per year and sometimes could reach \$3.8 million.¹⁵⁷ Such costs are high even for large companies. SMEs may not be able to routinely cover these compliance costs and could exit their respective markets, reducing consumer choices and discouraging innovation.

Some countries have considered or implemented data localization policies, such as mandated server localization or restrictions on where data can be processed. Stated motivations for these policies include the desire to ensure domestic privacy protections, or protect against foreign espionage. However these regulations are often inadequately articulated, vaguely construed and, therefore, nearly impossible to implement effectively.¹⁵⁸ In fact, rather than ensuring privacy or data security, forced localization creates a host of new valuable targets

for hackers. The rise of data localization mandates represents a costly and inefficient alternative to flexible and compatible privacy regimes.

The direct financial resources required to build individual data centers are immense. In 2013, it was reported that the average cost of building data centers in Brazil and Chile were \$60.3 million and \$43 million, respectively.¹⁵⁹ These sums are considerable even for large companies, and many SMEs would be unable to bear such costs. In addition, the ongoing burden of complying with these mandates would take the place of otherwise productive uses of capital.

It is not just Internet companies that are harmed by localization policies. These policies are likely to hinder broader economic development, rather than promote domestic industry. As a 2011 report notes, 75% of the value of the Internet accrues to traditional, non-Internet centric businesses through productivity gains and easier access to foreign markets.¹⁶⁰ As a result, such policies will invariably harm a wide swath of traditional domestic economic activity and harm a country's global competitiveness.¹⁶¹ Not surprisingly, economists at the European Centre for International Political Economy (ECIPE) found that current data localization proposals will have significant negative domestic economic effects on the countries that choose to adopt such regimes.¹⁶²

Perhaps more important than the economic costs of data localization and restrictive data protection regimes are their burdens on the Internet as a global platform for free expression. Such regimes can facilitate censorship through blocking access to services and platforms that do not comply with mandates to store or process data within a particular nation's borders, depriving consumers of a range of content and ideas to which they might otherwise have been exposed.¹⁶³

In addition to their significant adverse economic consequences, overly restrictive data protection and localization regimes can also violate trade obligations if applied indiscriminately or as a trade barrier in disguise. For example, Article XIV of the General Agreement on Trade in Services (GATS) ensures that member countries are not prevented from adopting measures designed to ensure compliance with laws protecting “. . . the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.”¹⁶⁴ However, this is subject to the requirement that such measures cannot be

arbitrary, discriminatory, or a disguised restriction on trade in services.

4. Developing Flexible Models of Data Protection

A number of countries have developed data protection regimes that permit cross-border data transfers with appropriate protections. No two systems are identical, but each attempts to strike the necessary balance between a responsible, principles-based framework to ensure consumer protection, and the flexibility to interface with regimes in other countries.

For example, Singapore implemented the Personal Data Protection Act (PDPA) in 2012, which permits an organization to transfer personal data overseas if the organization complies with data protection provisions and ensures that the data recipient is bound by enforceable obligations comparable to the PDPA.¹⁶⁵ Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) allows data transfers with the condition that “so long as the transfer is consistent with the use for which the data was originally collected, consent to transfer the data is not required.”¹⁶⁶ Meanwhile the U.S., while lacking a comprehensive privacy statute, instead has “a body of laws—a mosaic of federal and state statutes, common law jurisprudence, and public and private enforcement that obligate private entities to protect personal data and respect the rights of data subjects.”¹⁶⁷

Moving beyond domestic regimes, the new EU-U.S. Privacy Shield represents just one prominent example of an effective interoperable framework between nations. Other models exist around the world to promote similar functional compatibility between privacy and data protection laws with cross-border data flows. APEC has developed a voluntary Cross-Border Privacy Rules system (CBPR), which requires participating businesses to develop internal data transfer privacy rules consistent with the APEC Privacy Framework endorsed by APEC economies in 2004.¹⁶⁸ Demonstrating its interoperability with other regimes, APEC has also worked with the EU to streamline the application process for participating companies to use complementary data transfer mechanisms to operate in both regions.¹⁶⁹

It is important to recognize that interoperability need not require identity of data protection regimes. Indeed, even in the CJEU's decision invalidating the Safe Harbor Framework, the Court made clear that “the legal order of a third country need not be identical

to be deemed essentially equivalent to the EU data protection regime.”¹⁷⁰ Acknowledging that data protection regimes can achieve shared goals through different mechanisms is a key aspect of successful interoperable regimes.

5. Conclusion

The development of robust interoperable privacy and data protection regimes is vital to empowering consumers and businesses of all sizes to utilize the

vast commercial and connective power of digital technologies, while systems that unduly restrict data transfers across borders can have dire economic consequences. National laws and international frameworks should allow for the free flow of data crucial to e-commerce, while ensuring that data protections are strong enough to protect consumers effectively and maintain trust in the Internet as an accessible platform for expression, innovation, and global commerce.

Optimizing Societal Benefit of Emerging Technologies in Policy Development related to Data Flows, Data Protection and Trade

Joseph Alhadeff, Chair, International Chamber of Commerce Commission on the Digital Economy;
Chief Privacy Strategist, Vice President, Global Public Policy, Oracle Corporation¹⁷¹

The Internet, and the data flows that support it, has accounted for 15-20 percent of gross domestic product (GDP) growth in many countries, including developing countries.¹⁷² With the Internet of Everything (IoE) growing fast, machine-generated data are seen to contribute up to a projected 50-fold increase in Internet traffic between 2010 and 2020¹⁷³ with 1 trillion connected objects and devices on the planet generating data in 2015.¹⁷⁴ As data continue to be crucial to the functioning of the digital economy and the flourishing Information Society, appropriate policies and legal frameworks related to data protection and privacy are essential to assuring that consumers and citizens can continue to trust in engaging in transactions and using services online. Both privacy and security concerns need to be appropriately taken into account and policy frameworks should provide for robust and appropriate data protection that provides the needed trustful environment involving all players – guaranteeing the privacy of the citizen without hampering innovation.

Privacy is informed by cultural and legal frameworks as well as the subjective understanding and values of the data subject; even though laws and policies are written with the objective user in mind. At the level of general principles there is consistency on privacy approaches – Organisation for Economic Cooperation and Development (OECD) Guidelines, Council of Europe (CoE) Convention 108, Asia Pacific Economic Cooperation (APEC) Guidelines, European Union (EU) Directive 95/46, United States Fair Information Practice Principles (FIPPs) all are grounded in similar principles. The concept of privacy in application, however, varies between countries. Different jurisdictions have adopted various approaches to data protection that suit their jurisdictions that do not provide a harmonized implementation of the topic, creating potential problems of interoperability. This is especially the case for transborder flows of data, i.e. where data move from the country in which it is collected to other countries.

One of the most interesting projects advancing the concept of policy interoperability is taking place in the APEC Data Privacy Subgroup (DPS). The DPS has

been working with members of the Article 29 working group of the EU, as well as the European Commission and the European Data Protection Supervisor, to understand the potential policy interoperability between Binding Corporate Rules (BCRs) in the EU and Cross Border Privacy Rules (CBPRs) in APEC. The instruments serve similar purposes: both are designed to facilitate data flows while respecting applicable privacy requirements; both have controller and processor versions, and both require an application, vetting, validation and oversight process.

Before delving into the details of the project, it is useful to understand the difference between policy interoperability and mutual recognition. Policy interoperability focuses on finding and exploiting the commonality of the underlying principles and the way they have been implemented, in order to achieve operational and administrative simplification. Mutual recognition is the finding of complete interoperability that allows a finding of equivalence between systems. The APEC example will help clarify the concept.

The APEC DPS and EU representatives undertook a side by side comparison of the language of the instruments that enable BCRs and CBPRs. The created document called the “Referential” found that an approximately 70 percent overlap existed between the documents. That 30 percent gap means that mutual recognition is not appropriate as there is not an equivalence of requirements. There should however be a way to credit the common 70 percent that would create synergies and benefits of administrative simplification. There is also work underway to develop a common application so that those organizations wishing to do both at the same time may only have to complete one questionnaire and develop one set of proof documents related to the organization’s capacity to comply.

The more we can encourage consistency across the terminology, application processes and proof requirements, the more companies can free resources spent on administrative functions to be used for actual training, compliance and oversight. Our legal, cultural, societal and market differences are unlikely to yield

a unified privacy implementation, but interoperability can dramatically reduce administrative burdens while assuring that applicable privacy protections are maintained. There is also the benefit of improving the understanding and transparency of privacy requirements in practice and application across geographies, which is useful for service providers, users, regulators and policymakers.

Diverging policy regimes can also affect the accessibility and utility of emerging technologies. The Internet of Everything (IoE), machine-to-machine (M2M), cloud and big data analytics are having a profound economic impact that will reach \$3.9 trillion to \$11.1 trillion a year by 2025¹⁷⁵. McKinsey reports that at the top end, that level of value—including the consumer surplus—would be equivalent to around 11 percent of the world economy.¹⁷⁶ It is important therefore to consider how the absence of interoperability and compatible policy approaches can affect these potential benefits.

The combination of new and emerging technologies makes these concepts even more important. The potential for new analytics related to big data, cloud and the IoE to deliver new advances in medicine, health research, elder care, manufacturing and distribution, urban planning, sustainable development, education, environmental policies and sustainable consumption, just to name a few, is staggering. All of these uses however are predicated on the broader and more interconnected use of data, including personal data.

Personalized medicine, for many the holy grail of medical advancement, combines medical research and practice based on analytics of previously untapped personal and sensitive information. Today, doctors are ever more successful at identifying which drugs are most effective to treat ever-more granular subclassifications of diseases. Personalized medicine will enable doctors to not just understand which drugs are most effective to treat which diseases, but rather which drugs are most effective to treat the specific disease in a person taking into account genetic background, geographical/environmental condition and lifestyle characteristics. That requires more detailed and personal information than we collect today. Obtaining such information will require trust from data subjects and enhanced security from the holder of the information.

Small steps toward these ends are being taken, including work that both OECD and APEC are

conducting. OECD has recently worked on a framework that considers among other things the use of personal data in medical research. APEC is considering a project to make more productive use of previously collected medical information. The idea would be that where information was originally collected for medical treatment purposes, it might be impractical, if not impossible, to get a new consent for a medical or research use that was not consented to at the time of collection. Today ethical research protocols are used in medical research situations to control the use of the medical research data of a personal or sensitive nature. The APEC project would join these concepts with administrative simplification and more real time resolution of issues.

One of the major issues for researchers in the use of ethical research protocols is the time involved to establish and get approval for the protocol – six months or more in many cases. The APEC project would create an application template and have a defined protocol process which may regularize the procedure and limit some of the initial time and burden. The process would still require the disclosure and consideration of all relevant information similar to that at issue in today's processes. The major advancement is the creation of a library of models. If a model exists that is substantially similar to the research envisioned, then one could use the model as the template for the protocol and the inquiry would be limited to whether or not there is sufficient similarity in the research, scope and use to apply the model. This type of analysis could be undertaken in a matter of days or weeks but would not take months.

Another reason why such a library of use-based models might be interesting is because of the importance of correlation analysis in big data and analytics. Previously, models were predicated on developing questions to be asked across ever larger data sets with the hope of better answers from more data. Today, correlation analysis – finding patterns in the data itself without a specific question, but based on a term of parameter – means that the data may well inform the question we should ask. In a correlation model, traditional models of notice and consent are hard to apply. How can we provide notices of a specific purpose of collection and possible use if we don't know those facts until we query the data? Use models in conjunction with more generalized consents may help address the issues. The intent is not to lower the threshold of protection, but rather to consider methods of implementation and

practice that do not unduly constrain the potential benefits inherent in these new technologies. This is an area that requires more work across all stakeholders.

Another question that we will need to grapple with is data minimization. Data minimization requires that data not directly relevant to the purpose of collection are not collected. Today's analytics demonstrate that there may be great value in broader collection and retention. This is not without risk, however. The risk would arise from a compromise of the data or the use of the data for purposes not foreseen by or agreeable to the data subject. There are no quick answers to these questions, but it is clear that there should be ongoing efforts to explore innovative implementation of privacy laws and policies as well as new technical approaches to the safeguarding of information and the exercise of user choice and control. That being said, it is also important to note that in today's ever more complex data flows and value chains, making users responsible for granular control of data flows outside the relationship with the direct vendor represents an untenable burden. Concepts of fairness and equity must therefore come into consideration. Interestingly, the EU concept of Legitimate Interest has provided an interesting model for such a fair use analysis. ICC has recently published a paper on the topic that may also be of use¹⁷⁷.

The role of government access to data has also been an issue of growing importance. Recent work has been undertaken under the auspices of The Privacy Projects, which may be informative¹⁷⁸. Business is very interested in the proper resolution of these issues to bring greater certainty in how to manage obligations to both governments addressing national security issues as well as individuals whose privacy needs to be protected. Business encourages a broad and comprehensive dialog among governments to address these issues.

Another major trend which affects the ability to use information, including personal data productively, efficiently and effectively is data localization. Data localization can take many forms: keeping data within a country, requiring servers to be located in the country, stipulating requirements for local processing and requirements to use domestic technology, including locally created cryptography or algorithms. Data localization is often used to promote local industry or indigenous innovation. It can include technology mandates as well as technology transfer that encompasses the source code level. Data localization

eliminates many of the potential benefits and cost savings of cloud computing, returning in its most extreme form to more client-server oriented solutions or—in the less onerous case—to purely national cloud implementation. Such policies may result in diminished access to cloud resources as well as higher costs for those resources available. While localization may make the cloud more expensive for large players to provide and consume, it may make it completely unavailable to small and medium enterprises (SMEs), where a dynamically provisioned, use-only-what-you-need system may have the greatest multiplier effect. SME cloud services are often provided on larger provider's cloud platforms. Requirements that limit the attractiveness of such options may unduly constrain an entire operational group that accounts for some innovation, serves smaller niche markets, and creates local jobs. The very policies designed to boost local industry may well be its greatest constraint. This is also the case in countries that focus on mandatory requirements to provide cloud capacity locally as a growth strategy, where the greatest economic leverage comes from using rather than providing cloud services.

Data localization is sometimes rooted in justification of privacy or security. While business recognizes the need to comply with local laws, including those on privacy and security, they should be consistent with established trade rules and human rights¹⁷⁹. The General Agreement on Trade in Services (GATS) Article IX, which predated today's emerging technology, has laid out a number of the challenges in assuring that such limitations on the transborder flow of data be necessary, narrowly tailored, non-discriminatory and not a disguised trade barrier.

As privacy and security are growing concerns across stakeholders, parties will need to be able to demonstrate their capacity to comply with requirements for both. Countries will need to be able to demonstrate how they support compliance in law and practice and those transferring information will need to do the same, but across a broader range of instruments including contracts, practices and comprehensive privacy management programs¹⁸⁰.

Government regulation or 'top down' legislation may not be the most effective way to achieve an acceptable level of privacy protection. Heavy-handed privacy laws and regulations can have the unintended consequence of stifling innovation and growth. A broader dialogue is needed about how to assure the

correct level of protection of personal data while not creating limitations on innovative ways to implement such protections. This conversation must include all stakeholders as it will need to be supported by a basis of trust. Finally we must move from purely formulaic check box exercises of compliance (one-size-fits-all) to more outcomes based solutions that provide real and effective privacy protection while not constraining innovative uses of technology.

It is essential for governments to recognize tools for privacy protection developed by industry and to work together with industry to develop a privacy framework that both furthers privacy protection and promotes economic growth.¹⁸¹ In this context, the following steps may be considered as a starting point for governments to achieve optimum privacy protection and encourage international trade:

- Adopt a flexible and responsive approach to the protection of personal information, including the acceptance of a range of solutions (including codes and other non-legislative solutions) and technological innovations that empower the user, determining where specific laws are needed to protect individuals from harm and enact those laws in the most targeted fashion possible.
- Educate the public about privacy protection and the use of privacy-enhancing technologies¹⁸².
- Cooperate internationally to ensure an interoperable environment for different privacy regimes. In assessing the level of protection provided to personal information in other jurisdictions, the criterion should be the objective level of protection afforded by the system as actually used in practice with that jurisdiction¹⁸³.
- Government should avoid developing laws, policies and practices that create obstacles to transborder flows of personal data consistent with the applicable GATS obligations.
- Endorse model contracts, codes of conduct, seal programmes, and other non-legislative

mechanisms prepared by the private sector in order to promote the free and secure flow of information within and between companies across borders.¹⁸⁴

- Understand the importance of identifying and preserving benefit in the implementation of risk benefit analysis.¹⁸⁵

Conclusion

Further cooperation and effort is needed to develop practices aimed at ensuring protection for personal data that not only provides necessary protection of sensitive personal data and privacy, but also enables data driven innovations. Notably, the processing of appropriately de-identified data would give more flexibility to companies while still maintaining a high level of data protection. Similarly, use-based models with appropriate validation and oversight may provide useful tools to protect privacy where consent is not a viable option. Global cross-border data flows enable both economic growth and societal benefits. Any public policy limitation to these flows should be consistent with agreed GATS commitments and applied fairly to all actors in the information communication technology (ICT) economy. Where there are multiple ways possible of being compliant with data protection and privacy regulations, businesses should be able to use the least burdensome but equally efficient method of compliance. Trust and confidence in the availability, reliability, and resiliency of information systems and networks, including the Internet, must continue to be strengthened in order to realize ICT-enabled economic growth and ensure the seamless operation of global business.¹⁸⁶ All stakeholders must work together to promote effective data protection policies that protect users', keep up with societal needs, support innovation and promote international trade and investment.

Middle East and Africa (MEA)

Privacy Principles Will Protect Privacy and Advance Trade

The case for a new legal framework

Eduardo Ustaran, IAPP board member; *Olanrewaju Fagbohun*, Research Professor, Nigerian Institute of Advanced Legal Studies; *Yasin Beceni*, Managing Partner, BTS & Partners; and Lecturer; Istanbul Bilgi University; *Ussal Sahbaz*, Director, Think Tank – TEPAV; *Geff Brown*, Assistant General Counsel, Microsoft Corp.; *Marie Charlotte Roques Bonnet*, Director Microsoft EMEA; *Ed Britan*, Attorney, Microsoft Corp.; *Heba Ramzy*, Director Corporate Affairs, Microsoft Middle East and Africa.

1. Introduction

Today, global privacy conversations are driven by European law and policy. These critical conversations undoubtedly affect data management overall, mainly between the mature markets. However, the world finds itself on the leading edge of a transformative technological revolution being driven by the economic and societal benefits that derive from access to data and data analytics. Emerging Markets (EM) are racing with time to capture these benefits, but are being left out of an innovation dialogue that is largely occurring between mature markets. To help emerging markets find their voice and be heard in this global discussion, we need to focus on what is relevant and address some of the critical issues that impede economic development in the MEA region. The key will be developing a legal framework - something new – that speaks to the privacy issues that individuals are dealing with today, without creating barriers to trade. The goal of such a framework should be development of a balanced environment that protects both security and privacy while enabling data to be accessed and flow across borders.

Such a framework would incorporate the MEA privacy principles into national law and cloud policy to protect individual privacy, encourage trade and hasten the economic growth and social prosperity that derive from big data analytics.

Protect Privacy:

- The MEA privacy principles build on privacy concepts solidified under European law.
- The traditional notice and consent legal regime is outdated and does not work in the big data world. Use restrictions are the future.
- Data subjects should be empowered to manage their data and exchange data for value.
- The MEA privacy principles incorporate these privacy law developments and are drafted to be applicable to the many different markets in the MEA region, implementable by the private sector, and forward looking to support an innovation agenda.

Encourage Trade:

- A direct link exists between privacy laws and cross-border e-commerce.
- A sound privacy legal regime based on globally accepted principles is critical for businesses to be able to trust and allow data to flow to a market.
- Countries wanting to participate in the information economy and to allow for cross-border flows of data should implement the MEA privacy principles to ensure that local laws are interoperable with laws in other jurisdictions.

Hasten Economic Growth and Societal Benefits:

- Data scientists have invented new ways for computers to uncover insights through powerful new computing techniques. These techniques enable computers to undergo cycles of “learning” from experience in order to draw insights and patterns out of data.
- Many of the new benefits of big data originate from these techniques, which have significantly improved the capacity of computers to solve complex problems.
- Big data have the potential to spur global economies by fostering job growth, enhancing productivity, enabling cost-savings and improving efficiency.

- Big data learning techniques will soon be capable of delivering services that improve people's lives in previously unimaginable ways.
- Implementation of the MEA privacy principles will alleviate the privacy issues that raise major concerns and are a significant barrier to widespread adoption of the new computing technologies, the Internet of Things, and big data analytics that will bring about economic growth and societal benefits.

2. The proposed legal framework

Recognizing the need to protect individuals' privacy rights and the potential for data to drive economic and social prosperity, the following framework should guide national privacy laws, regulations, policies, and guidelines. This framework seeks to leverage the advanced technologies, data analytics and Internet of Things, while ensuring the safety and protection of data – today's most valuable currency. The framework includes:

General Principles

Focus on a development-balanced regulatory environment that will enable privacy rights to follow data wherever it goes around the world. This will encourage innovation, and use of data to address key fundamental issues that have been identified in the UN Sustainable Development Goals. Access to data, data analytics and insights should not be confined to the developed world, but should be made available in the developing world through the right practices, policies and regulatory frameworks.

Core Principles: these are critical components of the framework

Our proposed core principles should be incorporated into national laws to ensure that individuals are in control of their personal data (capital), have full view of where it resides and how it is used. Transparency is critical. Cloud Service Provider (CSPs) should be required to describe succinctly how they handle customers' data, disclose key information about their operations and requests to access data by law enforcement. Further, CSPs should implement reasonable and appropriate security safeguards in line with international standards as a means to demonstrate compliance and have the mechanisms in place to enforce these practices.

Key Points

- **Transparency:** Particularly concerning law-enforcement access and sharing with sub-processors.
- **Individual empowerment:** The ability to collect data should not be negatively affected. Rather, individuals should be given power over how data are used and the ability to add value to the information. The informational asymmetry between controllers and data subjects needs to be remedied.

3. Conclusion

- The MEA region finds itself at a key inflection point for a potential economic transition and greater participation in the global digital economy. The world is on the cusp of a computing revolution.
- The MEA region starts from a largely clean slate when it comes to privacy law. Filling in the blanks with the MEA privacy principles would be an important step toward moving MEA countries to the forefront of the digital economy and thereby improving lives across the region.

Appendix:

Privacy Principles Framework

General Principles

Effectiveness: Build a legal and institutional framework that is understandable, minimally bureaucratic, and realistically capable of achieving its policy objectives. This framework should impose workable requirements and be supported through a combination of education, oversight, and enforcement.

Responsible data practices: Encourage and guide regulators to promote responsible, socially beneficial uses of data while focusing their enforcement on processing of data that results in harms to individuals.

Technology neutrality: Address the risks of collecting and processing different types of digital data and be workable across changing technologies that collect and process data.

Proportionality: Impose obligations on organizations where the measures required to comply are commensurate with the risks of privacy harms.

Regulatory interoperability: Define and implement national norms and values, while promoting international data flows and facilitating international cooperation among national regulators.

Core Principles

Culture of Responsibility: Create a culture of responsibility among organizations that process personal data. All organizations must be able to demonstrate, using appropriate mechanisms, processes designed to mitigate privacy risks associated with the data they process. This applies whether the organization determines the purposes and means of processing the data (data controller) or processes the data only on behalf of another organization (data processor). It also applies regardless of where an organization transfers data or whether it engages other organizations to process the data.

Transparency: Require organizations to inform individuals, through a variety of tools designed to promote awareness in context, about what personal data are collected and for what purposes, when the data may be shared with third parties, and the individuals' rights with respect to their data.

Individual empowerment: Promote individuals' empowerment over uses of their personal data including, at a minimum, giving individuals the means: to express meaningful consent for data processing that presents risks of significant privacy harms; to access and correct their personal data; to restrict certain further uses of their data; to obtain a copy of their data in a usable format; and to seek redress against improper use of their data.

Encouraging responsible data flows: Facilitate intercompany and crossborder data flows that are protected through appropriate technical and legal measures and not otherwise prescribe the location of data.

Privacy by design: Encourage a principle of "privacy by design" that contributes to a culture of responsibility but does not prescribe specific requirements that stifle innovation.

Data security: Require organizations to implement reasonable and appropriate physical, technical, and organizational safeguards for personal data and demonstrate that they audit those safeguards. References may be made to recognized standards as a means to demonstrate compliance.

Allocation of responsibility: A data controller should remain primarily responsible for meeting privacy obligations and for providing redress to individuals. As long as a data processor merely processes data on behalf of a data controller, its responsibility is to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations. Allocate liability among organizations that process data within an ecosystem according to their demonstrated fault giving rise to the liability.

Enforcement: Enforce these principles in an efficient and effective way. Enforcement discretion should take into account the measures that the sanctioned organization has (or has not) taken to meet its privacy and security responsibilities.

Implementation Principles

Define privacy harms: Clarify what are serious privacy harms based on national privacy-related practices and international norms. Organizations should prioritize reducing risks of these privacy harms including through data protection impact assessments, enhanced security, de-identification techniques, and appropriate restriction on data processing.

De-identified data: Definitions of pseudonymized and anonymous data should allow organizations to clearly distinguish situations in which the new law applies (or not).

Children's data: Focus on additional protection for children through parental control.

Sensitive and biometrics data: Identify sets of data that present a high level of privacy risks and that should entail specific data protection.

Governments



The protection of data in Benin

Adjaigbe S. Rodolphe, Jurist, Researcher in Law Telecoms ICT;
Director, Studies and Research, Ministry of Communication and ICTs

1. Introduction

The Republic of Benin is a francophone country situated in Western Africa, member of the West African Economic and Monetary Union (WAEMU), the Economic Community of West African States (ECOWAS), and the African Union (AU).

Benin adopted law No. 2009-09 of May 22, 2009 on the protection of personal data for the Republic of Benin and has created a National Commission on Information Technology and Civil Liberties, tasked with overseeing compliance with the requirements for the protection of personal data. This law is being revised in order to comply with the ECOWAS Supplementary Act A/SA 1/01/10 on Personal Data Protection. Benin has not yet ratified the African Union Convention on Cyber Security and Personal Data Protection.

2. Difficulties associated with implementing a data protection regime

Implementing a data protection regime in the Republic of Benin is difficult for several reasons that include the lack of:

- a strong national policy regarding data protection;
- a strong cooperation between stakeholders that retain data, including those dealing with commercial, touristic, medical, judicial, agricultural, governmental, technological, financial, and educational activities;
- a national data center;
- interoperability between collection and processing systems;
- a legal and institutional framework for the protection of data in general, as opposed to personal data. (Benin is in the second term of the National Commission for Informatics and Liberties).

3. Difficulties associated with cross-border exchanges of data and e-commerce

Benin faces challenges with the cross-border data flows in the case of e-commerce and outsourcing activities. Difficulties associated with developing effective cross-border e-commerce are related to:

- the absence of national legislation concerning e-commerce development in key areas such

as the protection of data, consumer activities online, and cybersecurity. Legislation in these areas has been developed by the Ministry of Communication and ICT, but have not yet been put before Parliament for adoption;

- insufficient ICT infrastructure to support e-commerce activities;
- undeveloped online payment systems;
- lengthy adoption for mobile payment services such as Flooz and Mobile Money; and

weak outsourcing and subcontracting practices.

4. Effects on SMEs

SMEs are faced with a multitude of data protection regimes, making it complex for them to adjust and comply with other different data protection regimes. As a result, access to online markets is restricted and an attempted entry can waste resources. The data below regarding the use of computers and Internet by SMEs: show that smaller businesses are less likely to use ICT services. These factors combined act to discourage SMES from fully engaging in the information economy.

The following indicators were released by the Ministry of Communication and ICT in 2012:

- Proportion of businesses using computers: 69.9 percent
- Proportion of businesses using the Internet
 - 0-9 employees: 18.9 percent
 - 10-49 employees: 58.3 percent
 - 50-249 employees: 80 percent
- Proportion of businesses with a website
 - 0-9 employees: 3.7 percent
 - 10-49 employees: 26 percent
 - 50-249 employees: 60 percent

5. Conclusion

The development and adoption of a data protection regime in Benin is made difficult due to legal and institutional problems, and also problems related to infrastructure. It is therefore necessary to focus on putting in place a cooperative data protection framework.

Implementation of Data Protection Legislation – The Case of Ghana

Albert Antwi-Boasiako, Founder & Principal Consultant, e-Crime Bureau, Ghana

1. Background

Ghana's Data Protection Act (Act 843) was passed in May 2012. The Act effectively introduces a legal right to privacy to Ghanaian citizens and residents and provides legal protection for personal information. It further guarantees the right to privacy enshrined in Article 18(2) of the Ghanaian Constitution. Even though the Act was passed by Parliament in May 2012 and came into force on 16 October 2012, the Ministry of Communications only officially launched the legislation in November, 2014.

2. The Journey toward Implementation of the Data Protection Act, 2012 (Act 843)

The government organized an 11-member Governing Board in November 2012 to oversee the implementation of the Act. The board was chaired by a retired Supreme Court Judge and representatives from the *Commission on Human Rights and Administrative Justice (CHRAJ)*, the National Communication Authority (NCA), National Information Technology Agency (NITA) and the private sector.

Section 1 of the legislation calls for the creation and maintenance of the Data Protection Commission (DPC), which has a mandate to register Data Controllers and Data Processors (Section 27), develop and maintain Data Protection Register (Section 3), implement and monitor compliance of the Act (Section 3) and conduct public awareness (Section 86) among other considerations. The Commission remained 'operationally passive' for some time until it was officially inaugurated in November 2014. Apart from setting up the required infrastructure and framework necessary to implement the Act, financial challenges and other logistical constraints have been cited as the reason why the Commission could not engage actively with the public until the later part of 2014. Available records suggest the Commission was admitted to the international body of regulators in 2014.

The Commission became increasingly active in 2015. In early 2015, the Commission embarked on a *Know Your Rights* campaign. The Commission engaged directly with key stakeholders including ministries, government agencies, financial services players and other critical groups such as credit referencing bureaus. A number of different communication strategies were employed to encourage parties to register as Data Controllers and Data Processors. These included newspaper advertisements, television appearances, and various meetings and events. In addition, an innovative online registration portal and online register was launched by the Commission to facilitate the registration process. Nevertheless, the campaign was not hugely successful. The Commission could not reach a number of stakeholder groups because of financial and other logistical constraints. According to the Commission, the awareness campaign reached about seven million residents.

In January 2016, the Commission organized its first ever Data Protection Conference that attracted more than 600 participants, including practitioners, data protection experts, and Data Controllers and Data Processors from both Ghana and abroad to discuss best practices.

3. Country Situational Analysis with respect to Implementation of the Act

In order to effectively implement data protection legislation in a developing economy like Ghana, specific conditions need to be met.

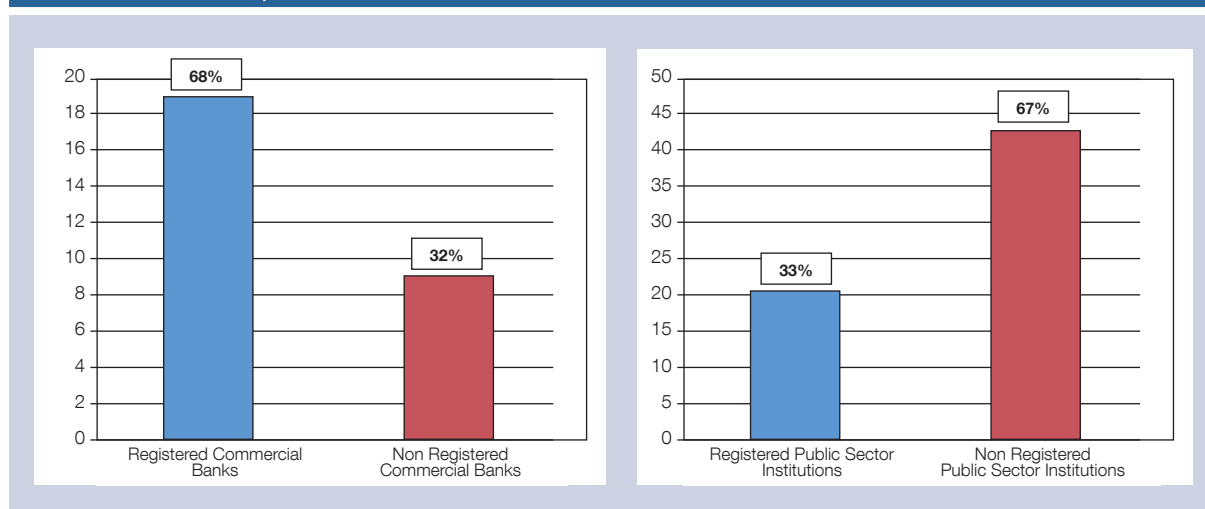
As part of this study, an in-country assessment was conducted in order to evaluate these conditions in Ghana. Analysis suggests efforts by the Commission to register Data Controllers and Data Processors focused on these key sectors:

Figure 1. Sectors considered for registration of Data Controllers & Data Processors by the Commission

Key Sector		Other Sectors	
1	Communication/Information Technology	1	Engineering
2	Education	2	Entertainment
3	Telecommunication	3	Manufacturing
4	Financial Services	4	Professional Services
5	Government	5	Real Estate/Housing
6	Health	6	Transportation/Tourism
7	Hospitality/Tourism	7	Informal Sector
8	Marketing	8	Energy
9	Mass Media	9	Mining
10	Security/Law Enforcement	10	Informal Sector/Others

In order to assess the success of the wide public campaign embarked upon by the Commission, two critical sectors were analyzed – the financial sector

and public sector organizations. The highlights of the findings on the status of registration by Commercial Banks and Public-Sector Institutions are shown below.

Figure 2. Comparative analysis of registration status of Commercial Banks and Public Sector Institutions as at December 31, 2015

Source: Ghana Data Protection Commission

A total of 28 commercial banks and 64 public-sector organizations comprising ministries, government agencies and law enforcement institutions were considered in the research. Registration status was verified from the online public register and in some cases, from follow-up calls made to some organizations to enquire about their knowledge of data protection registration obligations and/or their registration status. While commercial banks have a relatively high rate of registration (probably due to active involvement in the e-commerce industry), public sector actors lag. Government leadership is

important, since it can lead to increased compliance. According to Act 843, each government department is treated as a Data Controller (Section 91). This mandates all government institutions to register with the Commission. Our findings suggest only one-third of public sector institutions have registered with the Commission as compared with about two-thirds of commercial banks.

Even though the Commission has received some complaints about data breaches, they have not been actively prosecuted because of the need to create

awareness and also to develop the mechanisms to effectively implement enforcement actions including criminal prosecutions. For instance, under Act 843, a data controller who processes personal data without being registered would receive a fine up to 250 “penalty units” and/or up to 2 years of imprisonment. However, industry analysis suggests that fewer than ten percent of qualified Data Controllers and Data Processors have so far registered with the Commission, even though these institutions, including government ministries, departments and agencies, process personal data. Enhanced awareness and capacity-building among stakeholders—including prosecutors and judges—are needed in order to effectively enforce applicable sanctions under the Act.

On data localization, most businesses, including financial institutions, store their data outside of Ghana, because of the lack of adequate and reliable infrastructure—such as electricity—to manage data centers locally. However, the government has embarked on an ambitious project to reverse the trend by setting up a \$30 million National Data Center infrastructure. The infrastructure is expected to support in-country data storage for Ministries, Departments and Agencies (MDAs) as well as for private businesses.

Section 30 (4) of the Act mandates Data Controllers to ensure that data processed and stored abroad by Data Processors comply with the various regulations under the Act. Section 45 (2) of the Act also allows registration of external companies that collect personal information of Ghanaian residents as Data Controllers. These and other provisions ensures harmonization of the Act with other existing protocols within ECOWAS, specifically the ECOWAS Supplementary Act on E-Transactions A/SA.2/01/10 and ECOWAS Supplementary Act on Personal Data Protection A/SA.1/01/10). Ghana’s Data Protection Act also complies with the African Union (AU) Convention on Cyber Security and Personal Data Protection. The Act does not apply to data that originate externally and merely transit through Ghana.

4. Challenges, Lessons Learned and the Way Forward

The Data Protection Commission in Ghana faces several challenges and independent assessment suggests the Commission has performed quite well

despite the challenges. Some of the key challenges facing the commission include:

- *Human Resource/Financial/Logistical Challenges* – The Commission has been operating with a skeletal staff since the time of its inception. The law requires the Commission to develop certain competencies to be able to monitor and ensure compliance by Data Controllers and Data Processors but human and financial resources are affecting its operations. The Commission requires data protection, information security and privacy experts—among others—to be able to carry out its mandate under the Act. The Commission intends to rely on internally-generated funds to finance its activities.
- *Lack of Awareness* – Analysts have expressed concern about the lack of awareness about the existence, objectives and the relevance of the Data Protection Commission and its activities in general.
- *A Culture of Data Security* – In a jurisdiction, including Ghana, where citizens— both Data Subjects and Data Controllers/Data Processors—lack a culture of security, implementation of data protection measures including enforcement proves challenging.
- *Registration Costs* – Some businesses interviewed, including SMEs, complained about costs associated with registration with the Commission. In Ghana, there are three registration fee bundles, but most businesses are likely to pay 750 Ghana Cedis (GHS 750) which is the middle bundle. This is equivalent to about £130. Comparatively, in the UK it costs about £35 for most businesses to register. However, businesses with a turnover of £25.9M or more and public sector organizations with more than 249 employees pay a different fee. Despite this concern, income from the registration is seen as a critical financial resource base to sustain the operations of the Commission.
- *Government Commitment and Independence of the Commission* – Commitment by the state and its agencies is crucial to support data protection implementation measures. Even though the Commission is supposed to be an independent body, government through ministerial or agency interference is not enhancing the work of the Commission.

- *Enforcement* – Enforcement actions are required to ensure compliance with the Act. The Commission has given a strong indication of its preparedness to enforce sanctions in order to compel qualified Data Controllers and Data Processors to comply with the Act. The Commission intends to set up a Complaints and Investigations Unit by mid-2016 to facilitate its enforcement actions. The Commission is expected to recruit data protection and privacy experts to help investigate data protection breaches as part of its enforcement strategies.

On the way forward, government commitment and involvement in implementing data protection legislation is crucial; this is one of the lessons learnt from the study. The study has shown that awareness remains a critical factor affecting implementation of and compliance with data protection legislations. Awareness campaigns are seen as an important initiative in addressing data protection implementation challenges. It is recommended that, at the early stage of implementation of data protection legislations,

developing economies like Ghana should focus more on encouraging stakeholders and individuals to embrace data protection best practices through awareness programmes rather than activating immediate enforcement actions. Awareness is key to facilitate compliance and enforcement.

Data protection authorities should be equipped and resourced to develop their capabilities and core competencies in order to implement data protection programmes and strategies. The development and implementation of relevant infrastructure to ensure a sustainable data protection implementation roadmap is crucial. Knowledge sharing and transfer among countries is key to achieve this. Developing countries require support for policy guidance – on short term, medium term and long term sustainable data protection implementation strategies and institutional development policy. In enhancing awareness of data protection issues among the business community, data protection bodies should actively engage the business community and orient them toward making data protection and privacy a core business value.

The status of data protection in Mauritius

Ammar Oozeer, Barrister-at-law & Partner, Juristconsult Chambers

1. **Brief overview of the Data Protection law in Mauritius**

The Mauritius Data Protection Act (DPA)—to a large extent based on the E.U. Directive 95/46 on the protection of individuals with regard to the processing of personal data and free movement of such data—was passed on 1 June 2004. The DPA regulates the processing and cross-border transfer of personal data. Mauritius enacted the DPA in order to facilitate the development of Information Technology Enabled Service and Business Process Outsourcing (ITES/BPO) activities, especially originating from European companies. During parliamentary debates at the National Assembly in 2004, the then-Minister for ICT emphasized two objectives of the data protection law: first, to protect the personal data of individuals and second, to assure ITES/BPO operators that the personal data of individuals will be protected under the proposed law.

2. **Application of the DPA**

The DPA applies to a data controller (an individual or a group of person, whether corporate or unincorporated) who is established in Mauritius and processes data in the context of that establishment. A data controller who is established in Mauritius and uses equipment in Mauritius for processing data, other than for the purpose of transit through Mauritius, must also comply with the provisions of the DPA.

A person (an individual or a group of person, whether corporate or unincorporated) who is ordinarily resident in Mauritius, or carries out data processing activities through an office, branch or agency in Mauritius, is treated as being established in Mauritius and therefore that person must comply with the provisions of the DPA.

It must be emphasized that the DPA applies to a living individual who can be identified from the data that pertain to him or her.

3. **Personal data and sensitive personal data**

The DPA makes the distinction between ‘personal data’ and ‘sensitive personal data’. Personal data’ are: (a) data that relate to an individual who can be identified from those data; or (b) data or other information, including an opinion forming part of a

database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion.

More rigorous protection is provided to processing sensitive personal data, that is, personal data concerning the racial or ethnic origin, political opinion, religious or similar beliefs, membership of a trade union, physical or mental health, sexual preferences or practices, commission or alleged commission of an offence or proceedings for an offence of the data subject.

4. **Data controllers and data processors to be registered**

Data controllers and data processors must register themselves with the Data Protection Office. An application is made in writing to the Data Protection Commissioner (Commissioner).

5. **Data controllers obligations**

Unless an exemption applies, a data controller cannot collect personal data unless the collection (a) is for a lawful purpose connected with a function or activity of the data controller, and (b) is necessary for that purpose. At the time of collection, the data controller must inform the individual of certain information, for example (i) the fact that the data are being collected, (ii) the purpose or purposes for which the data are being collected, and (iii) whether or not the data collected shall be processed, and (iv) whether or not the consent of the data subject shall be required for such processing.

The data controller must ensure that personal data in his possession are accurate and up-to-date. Furthermore, a data controller cannot process the personal data of an individual unless the express consent of the individual has been obtained. In regards to the processing of sensitive personal data, the individual must have given his express consent to the processing.

The word “processing” is widely defined in the DPA. “[P]rocessing” is defined as any operation or set of operations that are performed on the data wholly or partly by automatic means, or other than by automatic means, and includes:

- collecting, organizing or altering the data
- retrieving, consulting, using, storing or adapting the data
- disclosing the data by transmitting, disseminating or otherwise making it available
- aligning, combining, blocking, erasing or destroying the data

Personal data may however be processed without obtaining the express consent of the individual if the processing is, for example, necessary (i) for the performance of a contract to which the data subject is a party, or (ii) for compliance with any legal obligation to which the data controller is subject.

If the purpose for keeping personal data has lapsed, the data controller must (i) destroy such data as soon as reasonably practicable, and (ii) notify any data processor holding such data that the purpose has lapsed and the personal data must therefore be destroyed. A data processor who receives such notification must, as soon as reasonably practicable, destroy the data specified by the data controller.

6. Rights of individuals (data subjects)

An individual may ask for information from a data controller about his personal data, the purpose or purposes for which the personal data are intended and if any disclosures have been made. The individual may also ask the data controller for a copy of any personal data held about him. When a request for information is made to a data controller, the latter must, except in specific circumstances, comply with such a request within a period of 28 days of the receipt of the request.

If an individual thinks that any personal data held about him by a data controller is incorrect, the individual may ask the data controller to rectify, block, erase or destroy such personal data.

7. Transfer of personal data to another country

Generally, the transfer of personal data outside Mauritius is prohibited unless the Commissioner has given her consent to such transfer. A transfer outside Mauritius can only take place if that third country ensures an adequate level of data protection. A full assessment is carried out by the Commissioner to determine if the third country provides adequate protection.

The transfer of personal data to a third country not ensuring an adequate level of data protection may take

place, for example, on the condition that the individual has given his or her consent unambiguously to the proposed transfer, or the transfer is necessary for the performance of a contract between the individual and the data controller, or for taking steps at the request of the individual with a view to his entering into a contract with the data controller.

The transfer of personal data to a third country may also be allowed on such terms as the Commissioner may approve for the protection of the rights of the individuals.

8. Enforcement

If the Commissioner is of the opinion that the processing or transfer of personal data by a data controller entails specific risks to the privacy rights of an individual, she may inspect and assess the security measures that the data controller is required to take under the DPA. The Commissioner may also carry out further inspection and assessment.

If a data controller or data processor has contravened, is contravening or is about to contravene the DPA, the Commissioner may serve an enforcement notice on the data controller or data processor requiring that certain remedial actions be taken within a specified time.

There may be circumstances where an investigation into a complaint discloses the commission of a criminal offence for which the assistance of the Police is needed. The matter is referred to the Police for further investigation.

According to the Fifth Annual Report published by the Data Protection Office that covers the period January to December 2013, the Data Protection Office enquired into 14 complaints in the following areas:

- (i) unauthorized viewing of personal images through the use of CCTV;
- (ii) unauthorized processing of fingerprint for attendance purposes;
- (iii) unauthorized access to personal data;
- (iv) unauthorized disclosure of personal data;
- (v) unsolicited messages; and
- (vi) unauthorized processing of personal data through fidelity cards.

It is worth noting that two decisions of Data Protection Office relating to the processing of fingerprints for attendance purposes were contested before the

ICT Appeal Tribunal. The Tribunal found in favour of the Data Protection Office. These two cases are on appeal before the Supreme Court however, and will be heard later this year.

9. Guidelines

Finally, it is worth noting that the Data Protection Office, in the discharge of its responsibilities under the DPA, has issued a series of guidelines that can be accessed on the website of the Data Protection Office. For example, guidelines have been issued in relation to the handling of privacy breaches, processing of personal data by video surveillance systems, privacy impact assessments and privacy enhancing technologies.

10. Reforms to the DPA

The ITES/BPO sector has grown from an emerging industry into one of the country's leading sources of employment and a major contributor to GDP. In order to tap more business opportunities from EU based companies, the National ICT Policy 2007-2011 proposed a two-pronged strategy:

- (a) to effect requisite changes in legislative and institutional domains with an objective of eventually bringing about an official recognition for Mauritius in the European Community as a "third country" whose data protection provisions are "adequate", and
- (b) concurrently, to evolve industry or sector-based codes of conduct that would merit recognition from respective countries on a case-to-case or a sector-to-sector basis.

In 2009, the Government of Mauritius requested accreditation from the European Union with regard to the adequacy of the data protection safeguards in Mauritius. In 2010, the Directorate General Justice of the European Commission commissioned a study on this issue. The Government of Mauritius requested technical assistance from the European Union in order to harmonize the Data Protection Act of Mauritius with EU standards on data protection as contained in the EU Directive of 1995 and other recognized international data protection principles and in keeping with the recommendations of the 2010 study.

The specific objectives were:

- (a) Remedy the gaps identified in the data protection legislation of Mauritius in relation to the EU standards namely about the:

- (i) Possibilities existing in Mauritian legislation that allow for the exemption of some activities not respecting the proportionality principle thus causing legal uncertainty;
 - (ii) The balance between the right to information and protection of personal data to be reassessed;
 - (iii) Contradictions in the legislation leading to restrictive protection of personal data.
- (b) Reinforce the institutional configuration of the Data Protection Office.

In her final report dated 9 December 2011, the EU consultant proposed amendments to be made to the Data Protection Act in light of the EU Data Protection Directive. Recommendations were also made on the optimal institutional structure for the Data Protection Office. For the purposes of the EU assignment, a national workshop was held to obtain the views of all stakeholders.

A draft Data Protection (Amendment) Bill that addresses the shortcomings found by the EU Directorate was prepared in 2012. The Bill has—unfortunately—not been introduced at the National Assembly to date.

Mauritius wants to reinforce its ICT- BPO sector to attract more EU based companies. To achieve this objective, Mauritius must ensure that its present data protection regime provides adequate protection for the EU companies and is in accordance with the EU Data Protection regime. It is therefore very unlikely that, at this stage, the country will consider signing and implementing the African Union Convention on Cyber Security and Personal Data Protection 2014.

Finally, it is worth noting that in November 2014, the Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108) had in its draft opinion recommended that the Committee of Ministers invite the country to accede to Convention 108. The few provisions of the DPA that the Consultative Committee has identified to be reviewed will, no doubt, be taken into account when amending the DPA. It is hoped that the amendments will be made soon, not only to comply with Convention 108 but also to be in accordance with the latest developments in EU data protection law. The objective of Mauritius is to create the right legal framework to attract ITES/ BPO operators to the country.

The status of data protection in Niger

Atte Boeyi, Director of Legislation, General Secretariat, and Ado Salifou Mahamane Laoualy,
Director of Judicial Affairs and Litigation

1. Background

Like many countries in West Africa, Niger is attempting to grapple with the digitalization trend. The trend presents many opportunities, but also introduces certain risks, particularly related to user confidentiality and privacy. Several Nigerien public agencies have endeavored to solve the problems associated with data protection, including the development of legislation.

The country has had the most complete draft legislation on ICT in the sub-region for many years. However, the complexity of developing and adopting legislation, along with a lack of national expertise, has caused delays in the development and implementation of laws. Some of the drafts need revision to ensure compatibility with regional e-commerce legislation.

Several challenges to the enactment and implementation of the legislation have been identified:

- 1) The implementation of data protection regulation calls for the involvement of several institutions, which do not prioritize the subject in the same way. This may lead to different expectations and levels of enthusiasm.
- 2) A lack of professionalism from those in charge of the treatment of personal data, including IT staff.
- 3) The illiteracy of the public, especially with regard to the dangers of violations of data privacy.
- 4) Citizens are not privy to the value and importance of data protection. Data protection and privacy are not widely seen as commercial products.
- 5) Users are not informed about data collection activities, or the purpose of such activities.
- 6) Modalities of data transfers, both domestic and international, are not defined.

Despite these difficulties and a need for cooperation of diverse stakeholders, progress is being made and legislation is being cooperatively developed.

2. Consumer Protection Law in Niger

In the area of consumer protection, Niger adopted a law in April 2015 reflecting the United Nations Guidelines for Consumer Protection, approved by the

General Assembly on 9 April 1985, through Resolution n39/248. Niger's adopted law thus tracks the same principles, and is applicable to all transactions and activities concerning the provision, distribution, sale, or exchange of goods and services. The governing principles include:

- The protection of consumers from hazards to their health and safety
- The promotion and protection of the economic interests of consumers
- Consumer education, including education on the environmental, social and economic impacts of consumer choice
- Availability of effective consumer redress
- High levels of ethical conduct for those engaged in the production and distribution of goods and services to consumers
- Promotion of sustainable consumption patterns
- The development of market conditions that provide consumers with greater choice at lower prices

The aforementioned law is already adopted and promulgated, and an implementing decree is currently being adopted. The law represents important progress for the protection of consumers in Niger.

3. Data Protection in Niger

The country is currently preparing a draft law on the protection of data, which draws on the OECD Guidelines, the European Directive on the Protection of Personal Data and the APEC Forum's framework for privacy protection. It should incorporate the ECOWAS A/SA.1/01/10 Supplementary Act on Personal Data Protection.

Niger has chosen to introduce data protection into the legal framework through a modification of the penal code. The modification will add data protection and cybercrime to the code currently not covered by the Penal Code adopted in 1961. The current draft is in the process of constitutional approval.

The Central Bank has also adopted a specific text in order to govern the activities of financial institu-

tions, especially payment and electronic transfer transactions.

Transnational and extra-territorial activities are governed by WAEMU and ECOWAS directives, which facilitate free circulation of goods and persons.

On the national level, the difficulty associated with the coordination of institutions and stakeholders is being resolved through the creation of a national committee, under the direction of the Prime Minister. This initiative seeks to transpose and implement the WAEMU and ECOWAS directives.

The legal and regulatory regime for data protection and privacy in Uganda

Denis Kibirige, Senior State Attorney, Ministry of Justice and Constitutional Affairs (MoJCA)

Barbarah Imaryo, Manager, Legal Services, National Information Technology Authority, Uganda (NITA-U)

1. Background

With the advent of information technology and the various challenges arising from it, including issues of data protection, the Ministry of Information and Communications Technology (MoICT) constituted a multi- sectoral team. Representatives from the First Parliamentary Counsel, the Ministry of Justice and Constitutional Affairs (MoJCA), the Uganda Law Reform Commission and the National Information Technology Authority, Uganda (NITA-U) were tasked with reviewing the current legal and regulatory framework. They were asked to address the issues of data protection and privacy aimed at creating a holistic and comprehensive legal and regulatory environment for the information technology (IT) sector. The review was also necessitated by the EAC Cyber Law framework Phase II, in which the Council of Ministers urged EAC member states to provide legal frameworks to include data protection and privacy among other issues.

Following the review, it was observed that there is currently no comprehensive law to safeguard the data collected or ensure that they are used only for the purposes for which they were intended. In many cases, the data collected are of a personal nature, which may easily be abused or misused in the absence of a legal framework to govern the integrity and circumstances relating to the use, storage and processing of data.

It is against this background that the proposal to develop the Data Protection and Privacy Bill, 2015 was premised.

2. Existing legal framework

In the absence of the comprehensive legal framework, data protection and privacy issues have been provided for in piecemeal in the following Laws.

- (a) Constitution of the Republic of Uganda
- (b) The Access to Information Act 2005 (Act No 6 of 2005)
- (c) The Uganda Communications Act, 2013 (Act No. 1 of 2013)
- (d) The Electronic Signatures Act, 2011 (Act No. 7 of 2011)

- (e) The Computer Misuse Act, 2011 (Act No. 2 of 2011)
- (f) The Regulation of Interception of Communications Act, 2010
- (g) Registration of Persons Act, 2015

3. Development of the Law

In developing the law, extensive research on and benchmarking of the legal and regulatory regimes and good practices on data protection and privacy in various jurisdictions globally was conducted. Its aim was to establish how data protection and privacy is regulated, and also to understand how compliance with the Law and various initiatives are being successfully achieved. Some of the jurisdictions include: Angola, Australia, Benin, Burkina Faso, Ghana, Malaysia, Mauritius, Morocco, Senegal, Singapore, Tunisia and United Kingdom.. Further, the African Union Convention on Cyber Security and Data Protection guidelines to Member States when developing legislation were considered and followed when developing the Bill.

4. Challenges encountered in the development of the law

Various challenges were encountered during the development of the Bill, such as:

- Limited Funding – the various stages of development of legislation have cost implications.
- Limited understanding of issues related to data protection and privacy – stakeholders who may be affected by the legislation and those required to implement it have limited understanding of and experience with the legislation, its purpose and what it seeks to achieve.
- Slow process of developing legislation – the process of developing legislation is protracted by the requirement to consult a wide range of stakeholders who will either be affected by the legislation or who will implement it. This requirement is aimed at building consensus in the legislation before formal introduction in the Cabinet and Parliament.

5. Status of the Bill

A draft Bill was presented to a wide stakeholders' forum on 27 November 2014. Preceding the stakeholder workshop, the draft Bill was posted on various websites for comments from the public and was discussed in various public fora to generate interest in the subject of the bill. The comments were incorporated in the revised Bill that was subsequently approved by Cabinet. The Bill was published in the Uganda Gazette on 20 November 2015 and will be tabled in Parliament for the first reading in 2016.

6. What will the law achieve once enacted?

The law on data protection and privacy is intended to provide mechanisms and measures for protection of personal data. These proposed mechanisms and measures will relate to any kind of breach of individual privacy that may arise from the gathering, processing, transmission, storage and use of personal data and ensure that any data processing, in whatever form, respects the fundamental rights and freedoms of individuals.

The proposed Data Protection and Privacy Bill is intended to complement the existing laws on electronic transactions, communications and access to information by providing for protection of data and privacy.

Once enacted, the proposed Law will achieve the following:

- a) give effect to Article 27 of the Constitution by providing for the protection of private and personal data;
- b) safeguard the interests of individuals whose information or data are gathered or collected by the Government, public institutions, private entities;
- c) provide for the rights of individuals whose data are collected and processed;
- d) provide for the regulation of collection, holding, processing and use of personal data;
- e) ensure that the rights of individuals during data collection and processing are upheld against the threats and attacks capable of compromising the rights or the information;
- f) provide mechanisms for redress and remedies in cases where rights of individuals are infringed;

- g) provide for administrative mechanisms for ensuring that the processing of personal data is conducted in accordance with the procedures set out in the law to ensure that the privacy of the information relating to individuals is protected; and
- h) provide the criteria for transferring data to a country outside of Uganda. The recipient country should have adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

7. How the proposed law will support the business process outsourcing and ITES sector

Over the past five years, the Business Process Outsourcing/Information Technology Enabled Service (BPO/ITES) industry has grown progressively and is increasingly recognized in Uganda. To date, there are about 100 BPO/ITES companies registered with the Uganda Business Process Outsourcing Association (UBPOA). However, the sector has faced a number of challenges, such as: failure to win contracts for processing personal data, especially in the health and banking sector (both offshore and onshore) and the absence of a comprehensive data protection and privacy law.

8. Conclusion

The Bill has received considerable support insofar since it aims to protect citizens' personal data from both the Cabinet and other stakeholders. Among BPO providers, the Bill has been long awaited because it will enable them to win more contracts from countries that have otherwise not been able to consider Uganda due to its lack of a data protection law.

It is also noteworthy that we received a lot of technical support from United Nations Conference on Trade and Development (UNCTAD) during the development of the Bill. UNCTAD has also pledged to render additional technical support in the briefing of Parliamentarians when the Bill is tabled before Parliament.

Once enacted, not only will it address the issues related to protection of the privacy of individuals, provide security for personal data, but also contribute to economic advancement for Uganda as a whole.

Privacy and security of personal data in the United States

Melinda Claybaugh, Counsel for International Consumer Protection and Hugh Stevenson,
Deputy Director of the Federal Trade Commission's Office of International Affairs, United States

1. **Short background on the United States privacy regime**

In the United States, the privacy and security of personal data is governed by a wide range of federal and state laws. At the highest level, the Fourth Amendment to the United States Constitution protects “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. In the regulatory sector, multiple federal agencies enforce various privacy laws tailored to specific industries, or types and uses of information. These laws include but are not limited to health information, financial information, educational records, children's information, and governmental use of personal data. The regulatory agencies tasked with their enforcement include but are not limited to the Federal Trade Commission (FTC), the U.S. Department of Health and Human Services (HSS), the Consumer Financial Protection Bureau (CFPB), and the Federal Communications Commission (FCC). There are also state level agencies, including State Attorneys General, that enforce state privacy laws. Some of these laws are modeled upon federal laws, while others go beyond federal law. Finally, in many instances there are private rights of action available to individuals to vindicate their privacy interests.

The FTC, an independent U.S. agency established in 1915, is the federal agency with primary responsibility over privacy and data protection in the commercial sphere. Its privacy activity is part of its overall mission to protect consumers. This response has been prepared by FTC staff and, accordingly, focuses on the FTC's jurisdiction and areas of expertise.

A. Federal Laws

The broadest federal law protecting the privacy and security of personal information is the Federal Trade Commission Act,¹⁸⁷ which confers broad authority to the FTC to combat “unfair or deceptive” commercial practices. The FTC relies upon the FTC Act to protect consumer privacy interests where deceptive and unfair business practices result in privacy violations. The FTC has used this flexible authority to address a number of data security and privacy practices, including those that emerge with the development of new technologies and business models.¹⁸⁸ The FTC's

consumer privacy enforcement orders do not just protect American consumers; rather, in appropriate circumstances they can protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.¹⁸⁹

In addition to the FTC Act, the FTC has the authority to enforce the following laws that protect and govern the use of personal information:

- **The Children's Online Privacy Protection Act (COPPA).**¹⁹⁰ This Act, along with its implementing Rule, protects children's privacy by giving parents the tools to control what information is collected from their children online. Under the Act, 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.

The Act was updated in 2013 to address new developments – such as social networking, smartphone Internet access, and the ability to use geolocation information – that affect children's privacy.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act).¹⁹¹ This Act establishes requirements for those who send unsolicited commercial e-mail. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial e-mail provide recipients with a method for opting out of receiving such e-mail and must be identified as an advertisement.

- **The Fair Credit Reporting Act (FCRA).**¹⁹² The FCRA, enacted in 1970, 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 permissible purpose to use the information. The FCRA also requires anyone using consumer reports for credit, insurance, or employment purposes to notify the consumers when adverse actions are taken on the basis of such reports. Further, consumers are entitled to have inaccurate or incomplete information on their credit reports corrected or supplemented.
- **The Telemarketing Sales Rule.**¹⁹³ The Rule prohibits sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry, and calling consumers after they have asked not to be called again.

There are additional federal privacy laws that apply to specific sectors including, among others, healthcare, banking, and communications. These laws are enforced by various agencies within the U.S. government.

Several of these key laws are set forth below.

- **The Communications Act of 1934, as amended.**¹⁹⁴ The Communications Act protects the privacy and security of consumer information collected by communications providers in the operation of their networks, including telecommunications carriers, Voice over Internet Protocol (VoIP) providers, and cable and satellite operators. The Act requires covered entities to protect the confidentiality of customers' personal information and limit its disclosure.
- **Electronic Communications Privacy Act of 1986.**¹⁹⁵ This law amends the federal wiretap law to cover specific types of electronic communications, such as e-mail, cell phones, private communications carriers, and computer transmissions. It also extends the ban on interception to the communications of wire or electronic communication services and sets restrictions on access to stored wire and electronic communications and transaction records.
- **Federal Privacy Act of 1974.**¹⁹⁶ This law applies to the access to, and disclosure of, records of individuals held by federal executive and regulatory agencies. It requires such agencies, with some exemptions, to limit disclosure, provide access to the individual, and to apply basic Fair Information Practice Principles to such records containing the personal information of individual U.S. citizens and legal alien residents.
- **Family Educational and Privacy Rights Act (FERPA).**¹⁹⁷ FERPA applies to educational agencies and institutions funded by the U.S. Department of Education. It protects the privacy of students' education records by requiring written permission from the parent or student in order to release information from a student's education record.
- **The Gramm-Leach-Bliley (GLB) Act.**¹⁹⁸ The GLB Act and its implementing regulations are designed to ensure that financial institutions protect the privacy of nonpublic personal information about consumers. Among other things, the Act and the regulations limit disclosures of such information by financial institutions to unaffiliated third parties, including marketers; and require financial institutions to regularly notify their customers about their privacy policies.
- **The Health Insurance Portability and Accountability Act of 1996.** HIPAA and its implementing regulations (together, "HIPAA")¹⁹⁹ provide federal protections for personal health information held by certain public and private sector entities, including health care providers. Among other things, HIPAA regulates the uses and disclosures covered entities may make of personal health information, and gives individuals rights with respect to such information, including the right to examine and copy their records. HIPAA also requires entities to implement administrative, physical, and technical safeguards to assure the confidentiality of electronic protected health information. In 2009, the Health Information Technology for Economic and Clinical Health Act extended certain of HIPAA's privacy and security protections to third-party contractors of entities covered by HIPAA.

B. State Laws

In addition to the federal laws listed above, there are also many state laws relating to privacy and protection of personal information, including laws governing website privacy policies, personal information held by Internet service providers, online marketing of certain products directed to minors, and employee e-mail monitoring.²⁰⁰ As just one example, the State of California, in addition to a state Constitutional right granting each citizen an “inalienable right to pursue and obtain privacy,” also has dozens of laws governing online privacy notices, digital privacy rights for minors, disposal of customer records, telecommunications privacy, wireless network security, and connected televisions, among many others.²⁰¹

Most of the fifty states have laws dealing with the privacy of health information and medical records (in addition to the federal law described above).²⁰² Also, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws requiring private, governmental, and/or educational entities to notify individuals of security breaches of personal information. These laws typically have provisions indicating who must comply with the law, defining “personal information,” specifying what constitutes a breach, and setting forth the requirements for notice.²⁰³

C. Codes of Conduct

In addition to the laws set forth above, many self-regulatory codes of conduct for privacy exist in the United States. In general, the FTC has viewed industry self-regulation as a useful complement to its regulatory tools. Potential advantages of self-regulation include: (1) the relative speed and flexibility with which such rules can be developed or adapted to changing circumstances (compared to laws) and (2) the fact that industry representatives may have the necessary specialized knowledge for developing appropriate standards for a given industry.

In the area of children’s privacy, the Children’s Online Privacy Protection Act (COPPA), described above, allows industry groups to submit for Commission approval self-regulatory guidelines that implement the protections of COPPA. These programs have primary responsibility for ensuring their members’ compliance with their requirements but members remain subject to enforcement actions by the FTC. The FTC has approved several COPPA safe harbor programs,

which together have more than 140 members with more than 1,100 sites and apps.²⁰⁴

The U.S. government has participated and will continue to participate in the development of various codes of conduct designed to increase international interoperability among various privacy regimes. These include the APEC privacy framework (and ancillary Cross-Border Privacy Rules System),²⁰⁵ the 2000 U.S.-EU Safe Harbor Framework,²⁰⁶ and the EU-U.S. Privacy Shield Framework.²⁰⁷ These interoperability mechanisms reflect principles of notice, choice, onward transfer, access, security, data integrity and accountability.

The use of such codes of conduct does not imply a lack of enforceability and oversight. Indeed, when a company misrepresents to consumers that it adheres to a self-regulatory code of conduct, the FTC may hold the company liable for such misrepresentations pursuant to the FTC Act.²⁰⁸

2. Main principles

As discussed above, the United States has a broad range of federal and state laws governing privacy, each with an approach to privacy tailored to the context of the law. This response addresses only the FTC’s approach to privacy in the commercial sector.

The FTC communicates its key privacy and data protection principles through policy statements and recommendations, business education materials, and enforcement actions. Key privacy elements promoted by the FTC include the following:

- “Privacy by design,” or promoting consumer privacy throughout organizations and at every stage of the development of products and services.
- Substantive privacy protections, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.
- Comprehensive data management procedures throughout the life cycle of products and services.
- Simplified consumer choice relating to data practices, including the ability for consumers to make decisions about their data at a relevant time and context.
- Transparent information collection and use practices.

- Reasonable access to the consumer data, with the extent of access being proportionate to the sensitivity of the data and the nature of its use.²⁰⁹

In recent years, the FTC has provided further guidance on implementing these principles, particularly in light of emerging and evolving technologies and practices. Such guidance has addressed privacy practices relating to: privacy disclosures on mobile devices; the Internet of Things; data security, including best practices for mobile app developers; Big Data analytics; and compliance with COPPA.²¹⁰ In addition to the FTC's published guidance, the agency provides interpretations of the key privacy principles – particularly in light of evolving business models and technologies – through its enforcement actions. Since 2002, the FTC has brought almost 60 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk. The FTC has also brought more than 40 general privacy lawsuits, and more than 20 cases alleging violations of COPPA.

3. Number of countries following the same regulatory approach

The legal landscape in the United States relating to privacy is unique because it has developed over decades within the country's specific historical and legal context. Nonetheless, the FTC's general approach to privacy is similar to approaches followed by various multinational fora, including the OECD, APEC, and the OAS. For example, through its reports, guidance, and enforcement actions, the FTC has supported the principles of collection limitation, security safeguards, accountability, support for self-regulation, data breach notification, and cross-border enforcement cooperation, which are all central to the 2013 OECD revised privacy guidelines.²¹¹ In addition, FTC requirements that businesses conduct continuous risk assessment and implement security measures commensurate to risk are key aspects of the 2015 OECD revised security guidelines. Similarly, privacy principles promoted by the FTC are consistent with the principles outlined in the APEC privacy framework and Cross-Border Privacy Rules (which themselves were modeled on the original 1980 OECD privacy guidelines). Finally, the FTC's guiding privacy principles align with the OAS Principles on Privacy and Personal Data Protection.²¹²

In addition to sharing such common core privacy principles, as an enforcement agency the FTC also shares a common focus with many privacy

enforcement agencies around the world. The FTC actively participates in international enforcement cooperation networks to enhance information sharing and cross-border collaboration on privacy enforcement matters. These networks include the Global Privacy Enforcement Network (GPEN),²¹³ the APEC Cross-Border Privacy Enforcement Arrangement (CPEA),²¹⁴ and the London Action Plan International Cybersecurity Enforcement Network (LAP).²¹⁵

Together, these multinational efforts reflect a commitment to many of the same high-level principles embodied in the FTC's framework – increased transparency and consumer control, the need for privacy protections to be built into basic business practices, and the importance of accountability and enforcement. They also reflect a shared international interest in having systems that work better with each other, and are thus better for consumers.

4. Challenges met in the implementation; in particular trade impact on consumers and enterprises

In our era of rapid technological change, all governments and regulators tasked with privacy and data protection face the same significant challenge: staying abreast of business and technical innovations that affect consumer privacy and data protection. As the chief privacy regulator in the United States, it is especially important that the FTC continually develop and enhance its technical expertise. Therefore, the FTC has created an Office of Technology Research and Investigation, which conducts expert research, advises on investigative techniques, and provides further insights to the agency on technology issues involving all facets of the FTC's consumer protection mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, Big Data, and the Internet of Things. The FTC also annually appoints a new Chief Technologist, who advises the Commission on evolving technology and policy issues.

Further, to analyze particularly complex or cutting-edge privacy issues more deeply, the FTC periodically hosts public workshops on specific topics. These workshops, which invite participation by consumer groups, industry, and academics, often inform subsequent guidance and enforcement actions by the FTC. In recent years, the FTC has hosted workshops on topics, including Big Data, the Internet of Things, cross-device tracking, and the most recent academic research on privacy topics.²¹⁶ The FTC also

shares knowledge and expertise with its enforcement counterparts around the world through international enforcement networks and bilateral relationships.²¹⁷

5. The pros and cons of adopting this regime for consumers and enterprises

The FTC approach to consumer privacy consists of enforcement under the FTC Act, policy initiatives, and robust business and consumer education. This multi-faceted approach benefits consumers by providing the FTC with a variety of tools to address a range of practices, including both persistent problems and new developments. In addition, the FTC's broad authority under the FTC Act provides a flexibility that allows the FTC to address emerging technologies and practices without seeking additional enforcement authority. The FTC's approach equally benefits businesses by providing guidance about the FTC's enforcement approach and creating avenues for industry input.

Under current U.S. law, the FTC has a broad mandate under the FTC Act to "prevent . . . unfair or deceptive acts or practices in or affecting commerce." There

nonetheless are two areas in particular where the FTC has advocated for additional powers to enhance its enforcement authority. Specifically, the FTC has called for federal legislation that would (1) strengthen its existing authority governing data security standards for companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.²¹⁸

6. Issues of harmonization across countries.

The FTC recognizes there is value in greater interoperability among data privacy regimes, as consumer data are increasingly transferred around the world. Meaningful protection for such data requires convergence on core principles, an ability of legal regimes to work together, and enhanced cross-border enforcement cooperation. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules.

NOTES

- ⁸² A 'global value chain' is the sequence of all functional activities required in the process of value creation involving more than one country. See Rashmi Banga; Measuring Value in Global Value Chains, p.6 http://unctad.org/en/PublicationsLibrary/ecidc2013misc1_bp8.pdf
- ⁸³ Kommerskollegium National Board of Trade; 'No Transfer, No Production-a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods', <http://www.kommers.se/In-English/Publications/2015/No-Transfer-No-Production/>
- ⁸⁴ Commonwealth Secretariat; 'The Commonwealth in the Unfolding Global Trade Landscape: Prospects, Priorities, Perspectives-Commonwealth Trade Review 2015', <http://thecommonwealth.org/commonwealth-unfolding-global-trade-landscape>
- ⁸⁵ OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>
- ⁸⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal L 281 of 23.11.1995] <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012>
- ⁸⁷ APEC; http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- ⁸⁸ These include the African Union Convention on Cyber Security and Personal Data Protection, ECOWAS Supplementary Act on personal data protection (A/SA.1/01/10), The 1981 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention No 108/1981, Strasbourg, 28 January 1981) and the APEC Privacy Framework.
- ⁸⁹ Brunei Darussalam, Fiji, Kiribati, Maldives, , , Nauru, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.
- ⁹⁰ Commonwealth Secretariat; Commonwealth Secretariat Strategic Plan 2013/2014-2016/2017, p.32. http://thecommonwealth.org/sites/default/files/page/documents/ComSec%20Strategic%20Plan%202013_2017.pdf
- ⁹¹ Commonwealth Secretariat; Report of the Commonwealth Law Ministers Meeting , 1980
- ⁹² Commonwealth Secretariat; Report of the Commonwealth Law Ministers Meeting, 1999.
- ⁹³ <http://thecommonwealth.org/sites/default/files/history-items/documents/Singapore%20Declaration.pdf>
- ⁹⁴ See more at 2/3-ways-cyber-crime-impacts-business.aspx?no_header_alt=true
- ⁹⁵ See Maria Grazia Porcedda, Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers Law 2012/25 Department Of Law.
- ⁹⁶ Commonwealth Secretariat; Report of the Commonwealth Law Ministers Meeting, 2002.
- ⁹⁷ Commonwealth Secretariat; Commonwealth Secretariat Strategic Plan 2013/2014-2016/2017, p.32. http://thecommonwealth.org/sites/default/files/page/documents/ComSec%20Strategic%20Plan%202013_2017.pdf
- ⁹⁸ See <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>
- ⁹⁹ 38 Commonwealth Member countries have been the beneficiaries of the ITU projects on the harmonization of Information and Communication Technologies (ICT) policies for enhancement of market competitiveness which definitely have affected privacy and data protection policies and legislation. <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx> .
- ¹⁰⁰ In 2008, the Economic Community of West African States adopted UNECA legislative Acts on cybercrime and personal data <http://www1.uneca.org> .
- ¹⁰¹ Additionally, the African Union Convention on Cyber Security and Personal Data Protection providing for the establishment of a credible legal framework for cyber security in Africa, adopted 27 June 2014 affirms a Resolution of the last session of the Assembly of Heads of State and Government of the African Union, and seeks to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion

and cybercrime control, <http://au.int/en/cyberlegislation>. This has implications for 17 Commonwealth Member States that form part of the African Union.

- ¹⁰² Many jurisdictions in the Asia Pacific region are participating in the development of the APEC Privacy Framework and related APEC Privacy Pathfinder Projects aimed at harmonized data protection legal infrastructure as well as those initiated by the Association of South East Asian Nations (ASEAN) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- ¹⁰³ United Nations, 'Small Islands Developing States', <https://sustainabledevelopment.un.org/topics/sids>.
- ¹⁰⁴ <http://data.worldbank.org/income-level/HIC>
- ¹⁰⁵ <http://data.worldbank.org/income-level/MIC>
- ¹⁰⁶ Commonwealth Secretariat; <http://thecommonwealth.org/sites/default/files/inline/ExecutiveSummarykeyfindingswayforward-CTR2015.pdf>
- ¹⁰⁷ <http://www.internetlivestats.com/internet-users/brazil/> (with more data on Internet use in Brazil).
- ¹⁰⁸ The landmark case is the crowdsourced law "Marco Civil da Internet" (the "Brazilian Internet Bill of Rights"). See: <http://foreignpolicy.com/2016/01/19/how-brazil-crowdsourced-a-landmark-law/>.
- ¹⁰⁹ In 2011, consumer protection was enhanced with the Credit Information Law (Law 12.414/11), which emphasizes transparency and control, rather than opacity and confidentiality. For an analysis of this law in relation with data protection, see Doneda, D, Schertel Mendes, L. (2014). Data Protection in Brazil: new developments and current challenges, in: S. Gutwirth et al, (ed), *Reloading Data Protection*. Springer.
- ¹¹⁰ <http://www.internetlegal.com.br/2011/04/governo-e-sociedade-discutem-anteprojeto-de-lei-sobre-protecao-de-dados-pessoais/>
- ¹¹¹ See the position of Brazilian Association of Marketing: <http://www.abemd.org.br/pagina.php?id=54>
- ¹¹² See <http://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf>
- ¹¹³ The original analysis is available at: <https://www.huntonprivacyblog.com/2015/02/06/brazil-releases-draft-personal-data-protection-bill/>
- ¹¹⁴ See <http://www.privacidade.net/?p=74> (analyzing the differences between the 2011 draft bill and the new one).
- ¹¹⁵ See <http://www.eudataprotectionlaw.com/data-portability/> (on data portability) and <http://www.olswang.com/eu-data-protection-reform/data-portability/> (commenting the 2012 European proposal).
- ¹¹⁶ For a study about the reactions of the private sector in the 2010-2011 public consultation, see Zanatta, R. (2014). A Proteção de Dados Pessoais entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. In: Newton de Lucca et al. (Org.). *Direito e Internet III: Marco Civil da Internet*. 1ed.São Paulo: Quartier Latin, p. 447-470.
- ¹¹⁷ <http://www.idec.org.br/em-acao/em-foco/proteco-de-dados-pessoais-nova-verso-de-anteprojeto-inclui-sugestes-do-idec-e-traz-avancos> (advancing the view that the new draft bill must be enacted).
- ¹¹⁸ An article produced by the International Comparative Legal Studies follows this reasoning: "Brazil does not have a specific a data protection regulatory authority, but the Ministry of Justice has performed similar functions in a series of cases involving the right to privacy, consumer databases and data breaches. The Ministry has recently created a National Secretariat with the scope of overseeing Internet relations that can endanger Brazilian consumers' rights in Internet services, including privacy issues, such as Sony's data breaches and Google's unified Privacy Policy". <http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/brazil>
- ¹¹⁹ emarketer.com, Global B2C E-commerce Sales to Hit \$1.5 Trillion This Year Driven by Growth in Emerging Markets. See: <http://bit.ly/1SPQrBc>
- ¹²⁰ *Ibid.*
- ¹²¹ [Evermerchant.com](http://evermerchant.com): E-commerce in real time infographic (archived). See: <http://bit.ly/1KRYhr9>
- ¹²² [Alizila.com](http://alizila.com) quoting research from Accenture & AliResearch See: <http://bit.ly/21e5upx>
- ¹²³ European Commission Consumer Conditions Scorecard 2015: <http://bit.ly/1V7oDK5>. The Scorecard also reports that, within the EU Single Market, cross-border e-commerce purchases are more common in smaller national markets, such as Luxembourg and Malta.

-
- ¹²⁴ TRUSTe, 2015 US Consumer Confidence Index. See: <http://bit.ly/1NIETKt>
- ¹²⁵ TRUSTe, 2015 UK Consumer Confidence Index. See: <http://bit.ly/1e51fJX>
- ¹²⁶ Ipsos Mori, Global Trends Survey, 2014. See: <http://bit.ly/1RGHLvG>
- ¹²⁷ European Commission, Special Eurobarometer, 359 - Attitudes on Data Protection and Electronic Identity in the European Union, 2011. See: <http://bit.ly/1TjkP5t>
- ¹²⁸ Econsultancy, Why do consumers abandon online purchases?, 2011 – See: <http://bit.ly/1QOoSSE>
- ¹²⁹ Symantec, Internet Security Threat Report, 2015. See: <http://symc.ly/1KlIm7>
- ¹³⁰ MacDonald and Cranor, 2008 The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue <http://www.is-journal.org>. Analysis calculated that it would take 76 working days to read every privacy policy an internet user encounters in the course of a year
- ¹³¹ UK analysis found that 43 percent of the adult English population would not be able to understand Google's 2013 terms and conditions. See: Luger, E, Rodden, T and Moran, S. - Consent for all: revealing the hidden complexity of terms and conditions, proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013. See: <http://bit.ly/1QhHv0C>
- ¹³² Turow, J, Hennessey, M and Draper, N, 2015 The trade-off fallacy - a report from Annenberg School for Communication, University of Pennsylvania. See: <http://bit.ly/1F4S958>
- ¹³³ Ipsos Mori, Global Trends Survey 2014. See: <http://bit.ly/1RGHLvG>
- ¹³⁴ World Economic Forum, Rethinking personal data: strengthening trust, 2012. See: <http://bit.ly/1XEMyMQ>
- ¹³⁵ Fast Company, Could Airbnb Create The “Verified ID” For the Sharing Economy? See: <http://bit.ly/1PA2QVO>
- ¹³⁶ Quantifying the economic benefits of effective redress, Colin Rule, University of Arkansas Law Review 2013. See: <http://bit.ly/245vG83>
- ¹³⁷ Ibid.
- ¹³⁸ Beldad, A., de Jong, M., and Steehouder, M. (2010), How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5). See: <http://bit.ly/1QDIM2D>
- ¹³⁹ The European Commission's Special Eurobarometer 431 on Data Protection (2015), found that Europeans have widespread concerns about the consequences of their data being misused. More than two thirds of respondents who feel that they do not have complete control over their personal data say they are concerned about this lack of control. See: <http://bit.ly/1HjvAil>
- ¹⁴⁰ For more examples, see Personal Data Empowerment: time for a fairer data deal? Citizens Advice UK (2015): <http://bit.ly/1XtrlBG>
- ¹⁴¹ For example, 'sticky policies' which are permissions that 'travel' with a person's data, communicating the terms on which they can be shared and with whom; and notifying that person's personal information management service when terms are broken.
- ¹⁴² Personal Data Empowerment: time for a fairer data deal? Citizens Advice UK (2015): <http://bit.ly/1XtrlBG>
- ¹⁴³ Bijan Madhani is Public Policy & Regulatory Counsel at CCIA. Jordan Harriman is a Policy Fellow.
- ¹⁴⁴ A list of CCIA members is available at <https://www.cciagnet.org/members>.
- ¹⁴⁵ The value of cross-border e-commerce could be as high as \$350 billion by 2025. In addition, the McKinsey Global Institute estimates that the share of total goods trade attributable to e-commerce grew from 3 percent in 2005 to 12 percent in 2013. See U.S. International Trade Commission, Recent Trends in U.S. Services Trade: 2015 Annual Report, May 2015, at 116, <http://www.usitc.gov/publications/332/pub4526.pdf>, and James Manyika, et al. Global flows in a digital age, April 2014, at 10, McKinsey Global Institute, available at http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age.
- ¹⁴⁶ Some studies indicate that cross-border e-commerce is more prevalent in developing countries than domestic e-commerce. More than half of B2C and C2C transactions in India and Singapore were cross-border in 2013, while the most online purchase by consumers in Colombia, Paraguay, and Venezuela is cross-border. See United Nations Conference on Trade and Development, Information Economy Report 2015 - Unlocking the Potential of E-commerce for Developing Countries, Mar. 24, 2015, at 15, http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf.
-

- ¹⁴⁷ See No Transfer, No Production, Sweden National Board of Trade, (2015) [hereinafter “Sweden National Board of Trade”], available at <http://www.kommers.se/Documents/dokumentarkiv/publikationer/2015/Publ-No-Transfer-No-Production.pdf>.
- ¹⁴⁸ Id at 13.
- ¹⁴⁹ See Joshua P. Meltzer, The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment 4 (Brookings Institute, Global Economy & Development Working Paper No. 79, 2014), available at <http://www.brookings.edu/~media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internettransatlantic-data-flows-version-2.pdf>.
- ¹⁵⁰ Id at 12.
- ¹⁵¹ Export.gov, U.S.-EU Safe Harbor Overview, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Feb. 12, 2016).
- ¹⁵² Department of Commerce International Trade Administration, Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor, available at https://business.usa.gov/exportportal?static/Safe%20Harbor%20Key%20Points%2012-2013_Latest_eg_main_068867.pdf.
- ¹⁵³ See Press Release, Article 29 Working Party, Statement on Schrems Judgement (Oct. 16, 2015), at http://ec.europa.eu/justice/data-protection/article-29/press-material/pressrelease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.
- ¹⁵⁴ See Michelle Gyves, German DPAs Announce Policy Severely Limiting Mechanisms for Lawful Germany-to-U.S. Data Transfers, Proskauer Privacy L. Blog, Oct. 26, 2015, <http://privacylaw.proskauer.com/2015/10/articles/european-union/german-dpas-announce-policy-severely-limitingmechanisms-for-lawful-germany-to-u-s-data-transfers/>.
- ¹⁵⁵ Matthias Bauer, et al., The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce, ECIPE (2013), available at https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_Ir.pdf.
- ¹⁵⁶ Susan Stone, et al., Emerging Policy Issues: Localisation Barriers to Trade, OECD Trade Policy Papers No. 180, 56 (2015), available at http://www.oecd-ilibrary.org/trade/emerging-policy-issues_5js1m6v5qd5j-en.
- ¹⁵⁷ Id.
- ¹⁵⁸ See Anupam Chander & Uyen P. Le, Breaking the Web: Data Localization vs. the Global Internet, UC Davis Legal Studies Research Paper No. 378, Apr. 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.
- ¹⁵⁹ Loretta Chao & Paulo Trevisani, Brazil Legislators Bear Down on Internet Bill Push for Data Localization, Wall St. Journal (Nov. 13, 2013), <http://online.wsj.com/articles/SB10001424052702304868404579194290325348688>.
- ¹⁶⁰ Matthieu Pélissié du Rausas et al., Internet Matters: The Net’s Sweeping Impact on Growth, Jobs and Prosperity, McKinsey Global Institute (2011), available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.
- ¹⁶¹ One possible example is that local SMEs in countries with forced localization mandates will be less attractive as partners for large companies, since they cannot receive personal data. See Sweden National Board of Trade at 15.
- ¹⁶² Matthias Bauer et al., The Costs of Data Localization: Friendly Fire on Economic Recovery, ECIPE (2014), available at http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.
- ¹⁶³ See Hosuk Lee-Makiyama, Protectionism Online: Internet Censorship and International Trade Law, ECIPE (2009), available at <http://ecipe.org/publications/protectionism-online-internet-censorship-and-international-trade-law/>.
- ¹⁶⁴ General Agreement on Trade in Services, WTO, Jan. 1995, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.
- ¹⁶⁵ See Sidley Austin, Singapore, The Privacy, Data Protection and Cybersecurity L. Rev. 212 (2014), available at http://www.sidley.com/~media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la___files/singapore/fileattachment/singapore.pdf.
- ¹⁶⁶ 2015 International Compendium of Data Privacy Laws, Baker Hostetler 31, available at <http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf>.
- ¹⁶⁷ Jacques Bourgeois, et al., Essentially Equivalent, Sidley Austin 132, available at <http://www.sidley.com/~media/publications/essentially-equivalent---final.pdf>.
-

- ¹⁶⁸ The Framework does not impose treaty obligations on member nations. Rather, it sets an advisory minimum standard and represents a consensus across member economies. See Sidley Austin, APEC Overview, The Privacy, Data Protection and Cybersecurity L. Rev. 19 (2014) available at http://www.sidley.com/~media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la___files/apec-overview/fileattachment/apec-overview.pdf.
- ¹⁶⁹ Angelique Carson, EU and APEC Officials Agree To Streamline BCR/CBPR Application Process, IAPP, May 26, 2015, available at <https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-brcrbpr-application-process/>.
- ¹⁷⁰ Essentially Equivalent at 149.
- ¹⁷¹ Mr Joseph Alhadeff's contribution to the UNCTAD study entitled Data protection regulations and international data flows: impact on enterprises and consumers goes beyond ICC positions in detail and example while still being generally consistent with agreed concepts in existing ICC positions and policy material. This contribution should therefore be considered as reflecting input from the Chair of the ICC Commission on the Digital Economy in his personal capacity rather than a wider reflection of ICC policy positions.
- ¹⁷² McAfee, Andrew and Erik Brynjolfsson, "Big Data: The Management Revolution" (2012).
- ¹⁷³ The International Data Corporation (2012). "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East." Sponsored by EMC Corporation. Available at www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf.
- ¹⁷⁴ IBM (2013). "IBM 2013 Annual Report." Available at www.ibm.com/annualreport/2013/index.html.
- ¹⁷⁵ http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
- ¹⁷⁶ Ibid
- ¹⁷⁷ <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2015/ICC-position-on-legitimate-interests/>
- ¹⁷⁸ <http://theprivacyprojects.org/systematic-government-access-project>
- ¹⁷⁹ P.27 <http://www.iccwbo.org/Data/Documents/Basis/Internet-governance/2015/ICC-BASIS-Key-messages-for-IGF-2015/>
- ¹⁸⁰ See: https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf
- ¹⁸¹ P.27 <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2011/ICC-EBITT-An-Inventory-of-ICT-Policy-Positions-and-Practical-Guidance-2nd-Edition/>
- ¹⁸² P.27 <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2011/ICC-EBITT-An-Inventory-of-ICT-Policy-Positions-and-Practical-Guidance-2nd-Edition/>
- ¹⁸³ Ibid
- ¹⁸⁴ Ibid
- ¹⁸⁵ <http://theprivacyprojects.org/wp-content/uploads/2015/04/Benefit-Risk-Analysis-for-Big-data-projects.pdf>.
- ¹⁸⁶ <http://www.iccwbo.org/Data/Documents/Basis/Internet-governance/2015/ICC-BASIS-Key-messages-for-IGF-2015/>
- ¹⁸⁷ 15 U.S.C. § 41 et. seq., available at <https://www.law.cornell.edu/uscode/text/15/41>.
- ¹⁸⁸ For examples of recent enforcement actions alleging unfair or deceptive practices in violation of the FTC Act, see the FTC's 2015 Privacy and Data Security update, available at <https://www.ftc.gov/reports/privacy-data-security-update-2015>.
- ¹⁸⁹ The FTC has the authority to seek legal remedies for any acts or practices involving foreign commerce that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct occurring within the United States. See 15 U.S.C. § 45(a) (4).
- ¹⁹⁰ 15 U.S.C. §§ 6501-6506, available at <http://www.ftc.gov/privacy/coppafaqs.shtm>.
- ¹⁹¹ 15 U.S.C §§ 7701-7713, available at <https://www.law.cornell.edu/uscode/text/15/chapter-103>.
- ¹⁹² 15 U.S.C. § 1681 et seq. as amended, available at <http://www.ftc.gov/os/statutes/031224fcra.pdf>.
- ¹⁹³ 16 C.F.R. § 310 et seq., available at <https://www.law.cornell.edu/cfr/text/16/part-310>.

- ¹⁹⁴ 47 U.S.C. § 151 et seq., available at <http://transition.fcc.gov/telecom.html>.
- ¹⁹⁵ 18 U.S. Code § 2510-2522, 2701-2711, 3121, 1367, available at <https://www.law.cornell.edu/uscode/text/18/2510>; <https://www.law.cornell.edu/uscode/text/18/2701>; <https://www.law.cornell.edu/uscode/text/18/3121>; and <https://www.law.cornell.edu/uscode/text/18/1367>.
- ¹⁹⁶ 5 U.S. Code § 552a, available at <https://www.law.cornell.edu/uscode/text/5/552a>.
- ¹⁹⁷ 20 U.S.C. § 1232g, available at <https://www.law.cornell.edu/uscode/text/20/1232g>.
- ¹⁹⁸ 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.
- ¹⁹⁹ Public Law 104-191; HHS regulations at 45 C.F.R. Parts 160 and 164; available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html>.
- ²⁰⁰ Links to state laws related to Internet privacy are available at <http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx>.
- ²⁰¹ A complete list of California's privacy laws is available at <https://oag.ca.gov/privacy/privacy-laws>.
- ²⁰² See <http://www.healthinfoweb.org/state>.
- ²⁰³ Links to state data breach notification laws are available at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.
- ²⁰⁴ More information about the COPPA safe harbor program is available at <https://www.ftc.gov/safe-harbor-program>.
- ²⁰⁵ Documents relating to the framework and the CBPR system are available at www.cbprs.org.
- ²⁰⁶ See <https://www.export.gov/safeharbor>.
- ²⁰⁷ See <https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield>.
- ²⁰⁸ For example, since 2009, the FTC has brought 39 enforcement actions against companies making misrepresentations about their participation in the U.S.-EU Safe Harbor Framework. Information about Safe Harbor actions brought in 2015 is available at <https://www.ftc.gov/reports/privacy-data-security-update-2015>.
- ²⁰⁹ These principles are further explained in "Protecting Consumer Privacy in an Era of Rapid Change," available at <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers> (2012).
- ²¹⁰ These guidance documents are available at: <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf> (mobile privacy disclosures); <https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things> (Internet of Things); <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> (data security); <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security> (mobile app security); <https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more> (Big Data); <https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report> (Big Data); and <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance> (COPPA compliance).
- ²¹¹ See <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.
- ²¹² See http://www.oas.org/en/sla/dil/newsletter_data_protection_IAJC_report_Apr-2015.html.
- ²¹³ Further information about GPEN is available at www.privacyenforcement.net.
- ²¹⁴ See <https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Enforcement%20Arrangement.pdf>.
- ²¹⁵ See <http://londonactionplan.org/>.
- ²¹⁶ Further information about these workshops is available at <https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion> (Big Data); <https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world> (Internet of Things); <https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking> (Cross-Device Tracking); <https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon> (academic privacy research).
-

²¹⁷ The FTC has Memoranda of Understanding with privacy enforcement authorities in Ireland, the Netherlands, and the United Kingdom.. Further information available at <https://www.ftc.gov/policy/international/international-cooperation-agreements>.

²¹⁸ Additional information on this subject is available at https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf.
