

Study Group 1 Question 6

Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks



Output Report on ITU-D Question 6/1

**Consumer information,
protection and rights: Laws,
regulation, economic bases,
consumer networks**

Study period 2018-2021



Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks: Output Report on ITU-D Question 6/1 for the study period 2018-2021

ISBN 978-92-61-34621-8 (Electronic version)

ISBN 978-92-61-34631-7 (EPUB version)

ISBN 978-92-61-34641-6 (Mobi version)

© International Telecommunication Union 2021

International Telecommunication Union, Place des Nations, CH-1211 Geneva, Switzerland

Some rights reserved. This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO licence (CC BY-NC-SA 3.0 IGO).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited, as indicated below. In any use of this work, there should be no suggestion that ITU endorses any specific organization, product or service. The unauthorized use of the ITU name or logo is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition". For more information, please visit <https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>

Suggested citation. Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks: Output Report on ITU-D Question 6/1 for the study period 2018-2021. Geneva: International Telecommunication Union, 2021. Licence: CC BY-NC-SA 3.0 IGO.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the

copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ITU or its secretariat concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall ITU be liable for damages arising from its use.

Cover photo credits: Shutterstock

Acknowledgments

The study groups of the ITU Telecommunication Development Sector (ITU-D) provide a neutral platform where experts from governments, industry, telecommunication organizations and academia from around the world gather to produce practical tools and resources to address development issues. To that end, the two ITU-D study groups are responsible for developing reports, guidelines and recommendations based on input received from the membership. Questions for study are decided every four years at the World Telecommunication Development Conference (WTDC). The ITU membership, assembled at WTDC-17 in Buenos Aires in October 2017, agreed that for the period 2018-2021, Study Group 1 would deal with seven Questions within the overall scope of “enabling environment for the development of telecommunications/information and communication technologies.”

This report was prepared in response to **Question 6/1: Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks** under the overall guidance and coordination of the management team of ITU-D Study Group 1 led by Ms Regina Fleur Assoumou-Bessou (Côte d'Ivoire), as Chairman, supported by the following Vice-Chairmen: Ms Sameera Belal Momen Mohammad (Kuwait); Mr Amah Vinyo Capo (Togo); Mr Ahmed Abdel Aziz Gad (Egypt); Mr Roberto Hirayama (Brazil); Mr Vadim Kaptur (Ukraine); Mr Yasuhiko Kawasumi (Japan); Mr Sangwon Ko (Republic of Korea); Ms Anastasia Sergeevna Konukhova (Russian Federation); Mr Víctor Martínez (Paraguay); Mr Peter Ngwan Mbengie (Cameroon); Ms Amela Odošić (Bosnia and Herzegovina); Mr Kristián Stefanics (Hungary) (resigned in 2018) and Mr Almaz Tilenbaev (Kyrgyzstan).

The report was authored by the co-Rapporteurs for Question 6/1 Ms Archana Goyal Gulati (India) and Ms Elisa Vieira Leonel (Brazil) in collaboration with Vice-Rapporteurs: Ms Caecilia Nyamutswa (Zimbabwe); Mr Mehmet Alper Tekin (Turkey); Mr Issouf Soulama (Burkina Faso); Mr Edva Altemar (Haiti); Mr Laith Draghmeh (State of Palestine); Mr Issiaka Alhabibou (Mali) and Mr Jinqiao Chen (China) who served as Rapporteur until 2020.

Special thanks go to chapter coordinators for their dedication, support and expertise.

This report has been prepared with the support of the ITU-D study group focal points, the editors as well as the publication production team and ITU-D study group secretariat.

Table of contents

Acknowledgments	iii
Executive summary	vii
Abbreviations and acronyms	x

Chapter 1 - Consumer protection in telecommunications/information and communication technologies (ICTs): Institutional framework..... 1

1.1 Global updates of consumer protection and empowerment mechanisms in policies, laws and regulations	1
1.2 Institutional reforms at international level, international organizations and associations, and global and regional cooperation: What is their role in consumer protection, and what are some of the new developments?	3
1.3 Institutional reforms at the national level among different countries relative to consumer protection. Role of national regulatory authorities and other relevant authorities in consumer protection	4
1.3.1 National monitoring, evaluation and enforcement mechanisms: Effectiveness of such measures - What can NRAs do? How to cooperate with industry? Which other players should be considered?	7
1.3.2 Capacity building: Digital skills and competency for regulators.....	9
1.3.3 Awareness-raising mechanisms that can be used by policy-makers and regulators (campaigns, services, etc.).....	10
1.3.4 Looking to the future: Collaborative regulation between policy-makers and regulators, between different regulators, between regulators and industry, and between regulators and consumer associations, both within the ICT sector and across other sectors	11

Chapter 2 - Consumer evolution: New challenges in a digital world13

2.1 Introduction	13
2.2 New business models (infrastructure, content and applications).....	14
2.3 The changing requirements of consumer protection in era of converged services	15
2.4 The main future challenges: Consumer trust and security	16
2.4.1 Privacy and consumer protection (digital identity, protection of personal data, privacy issues)	16
2.4.2 Trust in security in the use of digital services	20
2.4.3 Ethics (address best practices in the public and private sectors as well as in new contexts such as AI)	20

2.5 Conclusion: Collaborative regulation, international cooperation and consumer education.....	21
---	----

Chapter 3 - Shaping a new framework for ICT consumer protection in the digital ecosystem23

3.1 Protection vs innovation - How to protect consumers while still fostering innovation.....	23
3.2 Customer care (new technologies to facilitate customer experience).....	25
3.3 How to resolve problems arising from cross-border activities	28
3.4 How to meet the needs of persons with disabilities and of women and children in a new digital ecosystem (technologies, services and products focusing on consumer protection and digital literacy relating to consumer protection)	30
3.5 AI, IoT and other emerging technology users: A new category of activities and players needing new tools.....	32

Chapter 4 - Fostering consumer empowerment and awareness (competition, business models and prices, and transparency).....34

4.1 How can consumers be empowered to participate in the digital economy?	34
4.2 Transparency as a mechanism to promote competition on tariffs and quality of service	35
4.2.1 Comparison tools for transparency and consumer empowerment	35
4.2.2 Concrete examples of how regulators can raise awareness and communicate results of performance-monitoring exercises and consumer assessments to consumers (to keep consumers and users informed about the basic features, quality, security and rates of various services being offered by operators)	37
4.3 How can consumers defend their rights more effectively (concrete examples of mechanisms to protect consumers on selected issues enabling them to know and exercise their rights, to use the services properly, and to make informed decisions when contracting services)	38
4.3.1 Means to prevent fraudulent, deceptive and unfair commercial practices, transparency and subscription agreements	38
4.3.2 Best practices and tools to empower users/consumers and raise awareness on how they can manage their personal data	39
4.3.3 Mechanisms/means put in place by regulators so that operators/service providers publish transparent, comparable, adequate, up-to-date information on, inter alia, prices, tariffs, and expenses related to contract termination, and accessing and updating telecommunication services in order to keep consumers informed and to develop clear and simple offers as well as best practices for consumer education.....	40

4.3.4 Identification of best practices for national regulators and operators in the use and management of national telephone numbering resources	40
Chapter 5 - Conclusions and guidelines.....	41
5.1 Conclusions	41
5.2 Guidelines	42
Annex 1: Summary of contributions submitted to Question 6/1	43
Annex 2: Outcomes of the ITU Global Symposium for Regulators in 2018 and 2019 (GSR-18 and GSR-19).....	54

Executive summary

This report contains the results of the study of ITU Telecommunication Development Sector (ITU-D) Question 6/1 (Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks) for the study period 2018-2021.

The report comprises five chapters, covering the evolving regulatory and institutional framework for consumer protection in telecommunications/information and communication technologies (ICTs), including global updates and the implications of reforms at the international, regional and country levels; consumer evolution in the wake of new digital world challenges; the formulation of a new framework for ICT consumer protection in the digital ecosystem; fostering consumer empowerment and engagement; and conclusions and guidelines.

The content of the chapters is based on written contributions from ITU-D members who participated in the meetings under the Question and meetings of ITU-D Study Group 1, representing ITU Member States, Sector Members and Academia, as well as on the content of the webinar hosted under the Question on 2 July 2020,¹ which supported the formulation of an annual deliverable released in December 2020.² Many contributions were of a case-study nature. An overview analysis of the case studies is made in Annex 1 to the report, backed up by more specific analysis in the chapters to which each case study is particularly relevant. An effort was made to draw on every contribution submitted in compiling the report. The report formulates critical findings in Chapter 5 and offers guidelines that can be adopted by Member States, Sector Members and telecommunication/ICT service providers.

Lessons learnt

- The nature of consumer protection in the area of converged services has changed and will continue to do so because of rapid technological progress, the emergence of new services and their widespread uptake.
- The traditional telecommunication market is transforming into a new complex digital world, where bundling of products and services from different markets is becoming the norm.
- The new digital world requires national regulatory authorities (NRAs) to collaborate closely with other authorities, such as consumer-protection institutions, data-protection agencies, competition authorities and all other relevant organizations within the country in order to cover all new digital and innovative services.
- Consumer-protection principles and policies as well as recommendations and standards adopted at the international and regional levels can guide policy-makers and regulators at the national level, especially in an increasingly interconnected world.
- Institutional and international cooperation between NRAs around the world can be an important means to strengthen the capacities of digital consumers by sharing experiences and good practices. This has become even more evident from the COVID-19 response.
- As uptake of telecommunications services increases, unsolicited commercial communications or nuisance calls is emerging as a cross-border issue, with no global statistics from institutional sources at present.

¹ ITU-D. ITU Webinar on [Unsolicited Commercial Communications / Nuisance calls: Are consumers more vulnerable in the era of COVID-19? 2 July 2020.](#)

² ITU-D Study Group 1. Question 6/1. Annual Deliverable 2019-2020. [Unsolicited Commercial Communications - an overview of challenges and strategies.](#)

- Regulatory frameworks need to be based on striking the right balance between the interests of operators/service providers and users in areas such as subscription agreements, protection of intellectual property rights and the management of digital rights, without affecting innovative models of e-commerce.
- One of the key challenges for regulators is to establish a culture of security that promotes trust in telecommunication/ICT applications and services, while effectively enforcing privacy and consumer protection.
- Irrespective of the economic sector in which artificial intelligence (AI) and Internet of Things (IoT) are operating, transparency for the consumer arises as a central question. This point revolves around knowing which data are being collected, when, and how they will be used in the future.
- Personal data protection, privacy, the right to information, ethical billing, fair contract clauses, number portability, universal access, confidentiality, speedy complaint resolution, quality of service, radiation protection, child online protection, fair advertisements and the safe use of the Internet are key elements of any laws that seek to protect consumers.
- The deployment of new technologies and the introduction of new services have increased the demand for numbering resources. This has raised the need for an adequate National Numbering Plan for effective competition and to meet future demands.
- The regulatory approach with respect to the assignment, allocation, withdrawal and use of numbers, creating the possibility for number portability and carrier selection, should enhance competition in telecommunication markets.

Recommended guidelines

Some of the important recommended guidelines emanating from the study are:

- Protection of consumers from online fraud and the misuse of personal data should be an integral part of regulatory policy.
- Consumer education on rights and obligations should be at the centre of policy-making.
- Since the digital economy is borderless, there is a need for cross-border cooperation among regulators.
- Regulators need to exercise caution so as to avoid hindering innovation and growth of digital services.
- Investment in connectivity in rural and remote areas is now critical to enable individual and household connectivity, as pandemics and natural disasters can prevent people from getting access to broadband services through communal access points.
- Robust data-protection frameworks should be put in place if unwanted calls and unsolicited communication are to be minimized.
- Cross-sectoral collaboration should be encouraged along with revisiting regulatory approaches, such as co-regulation and self-regulation. This could lead to new forms of collaborative regulation based on common goals, such as social and economic good and innovation.
- Policy and regulation should be based on consultation and collaboration. In the same way that digital cuts across economic sectors, markets and geographies, regulatory decision-making should include the expectations, ideas and expertise of all market stakeholders and players, including academia, civil society, consumer associations, data scientists, end users and relevant government agencies from different sectors.
- Policy and regulation should be evidence-based. Evidence is critical for creating a sound understanding of the issues at stake and identifying the options going forward as well as assessing their impact. Appropriate authoritative benchmarks and metrics can guide regulators in rule-making and enforcement, enhancing the quality of regulatory decisions.
- Policy and regulation should be outcome-based in order to address the most pressing issues, such as market barriers and enabling synergies. The rationale for any regulatory

response to new technologies should be grounded in the impact on consumers, societies, market players and investment flows as well as on national development as a whole.

- Policy and regulation should be incentive-based, rewarding players who uphold consumer protection.

Finally, setting up institutions such as consumer education centres, dedicated consumer complaint-handling centres or commissions and setting up dedicated consumer courts is recommended in order to protect consumers effectively.

Abbreviations and acronyms

This table contains abbreviations/acronyms relating to international, regional or supranational bodies, instruments or texts, as well as technical and other terms used in this report.

Abbreviations/acronyms of national bodies, instruments or texts are explained in the text relating to the country concerned, and are thus not included in this table.

Abbreviation	Term
AI	artificial intelligence
ASEAN	Association of Southeast Asian Nations
ATU	African Telecommunications Union
BDT	ITU Telecommunication Development Bureau
BEREC	Body of European Regulators for Electronic Communications
BEUC	European Consumer Organization (<i>Bureau Européen des Unions de Consommateurs</i>)
BFM	billing feedback message
CERRE	Centre on Regulation in Europe
CI	Consumers International
CLI	calling-line identity
CoE	ITU centre of excellence
COP	child online protection
COVID-19	Coronavirus pandemic 2019
DFS	digital financial services
EC	European Commission
EDPB	European Data Protection Board
EECC	European Electronic Communications Code
EU	European Union
GDPR	EU General Regulation on Data Protection
GKO	Global Kids Online (UNICEF initiative)
GSMA	GSM Association
GSR	Global Symposium for Regulators
H2M	human-to-machine
ICN	International Competition Network

(continued)

Abbreviation	Term
ICPEN	International Consumer Protection Enforcement Network
ICT	information and communication technology
IMR	international mobile roaming
IOA	International Ombudsman Association
IoT	Internet of Things
IPTV	Internet Protocol television
ISP	Internet service provider
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
IXP	Internet exchange point
LDC	least developed country
M2M	machine-to-machine
NEF	New Economics Foundation
NGN	next-generation network
NGO	non-governmental organization
NRA	national regulatory agency
OAS	Organization of American States
OECD	Organisation for Economic Development and Co-operation
OTT	over-the-top
RED	Regional Economic Dialogue
RRA	regional regulators association
QoS	quality of service
SIM	subscriber identification module
SMEs	Small- and medium-sized enterprises
SMS	short messaging service
SNS	social networking service
TSP	telecommunication service provider
UCC	unsolicited commercial communications

(continued)

Abbreviation	Term
UNICEF	United Nations Children's Fund
UNCTAD	United Nations Conference on Trade and Development
USSD	unstructured supplementary service data
VAS	value-added service
WB	World Bank
WSIS	World Summit on the Information Society
WTDC	World Telecommunication Development Conference

Chapter 1 – Consumer protection in telecommunications/information and communication technologies (ICTs): Institutional framework

Drastic changes in the telecommunication/ICT sector as a result of digitalization and technological improvements have resulted in the necessity to review traditional consumer rights regulations based on basic ICT services and suppliers. The digital transformation that is under way in economies and societies has provided consumers with a wealth of commercial opportunities, while also bringing a number of new and emerging risks. For instance, in this new ICT environment, digital risks and lack of trust have become one of the most common reasons that consumers with access to the Internet do not use some digital technologies and applications and do not engage in online transactions. Similarly, many consumers fear that their personal information might be misused or that they might become victims of online fraud. More than half of the world's population still does not have access to the Internet.

Suggesting an adequate regulatory framework to facilitate digital transformation requires a clear understanding of the concerns that consumers experience and the extent to which these concerns are already addressed by existing law, as well as the gaps in the present legal regime that may cause an imbalance to the disadvantage of consumers.

Thus, new technologies in the telecommunication industry are usually accompanied by challenges that can only be addressed by all stakeholders in the industry. As a result, consumer policy-makers have recognized the need to do more to keep up with the pace of change inherent to digital transformation and to provide consumers with well-tailored protections and the tools that would enable them to participate effectively in the digital era; and governments around the world have put the task of consumer protection and empowerment in the digital world firmly on their agendas.

1.1 Global updates of consumer protection and empowerment mechanisms in policies, laws and regulations

Today, digital has become central to economies and societies, transforming the way people and societies live, work and interact. For consumers, too, interacting with information and data as well as accessing and benefiting from economic opportunities and doing business has also changed. With the accelerating digitalization of social and economic activities, data – and especially consumer data – are increasingly becoming a core driver of digital innovation and digital transformation.

The telecommunication sector is in a transitory period, and digital services are increasingly substituting traditional telecommunication services, such as voice telephony and SMS. It is expected that fundamental changes in telecommunication-sector regulations might be required

in the near future.¹ However, the changes that we have been experiencing recently also call for some incremental changes in current telecommunication regulations themselves.

In order to promote a symmetric, level playing field between traditional operators and new service players (such as OTTs) and at the same time increase choice for consumers with lower prices while providing high-quality and innovative services, legislations and regulations are currently under review in many countries.

Among others, the European Union (EU) has updated the EU's rules for electronic communication services and published its new European Electronic Communications Code (EECC).² EECC and the new BEREC Regulation entered into force on 20 December 2018. EECC includes new consumer-protection rules in different areas, such as non-discrimination, information, transparency, provider switching, portability, universal service and availability. It requires service providers to provide a summary of contracts to consumers. In addition, EECC enables consumers to terminate all elements of the service package when there are grounds to terminate any element of a bundle of services due to lack of conformity with the contract or failure to supply. From a consumer-protection perspective, it is expected that the new rules will serve to increase choice with lower prices, enhance security and confidentiality of communications, and provide high-quality and innovative services.

The regulation of online content has also attracted the attention of governments. Increasingly, regulatory measures are being examined, ranging from the adoption of self-regulation by intermediaries/platforms and the regulatory enforcement of a code of ethics to imposing liability to screen out harmful content. It is being considered whether new regulators need to be set up for this purpose. These bodies would also receive and settle consumer disputes and enforce accountability measures.³

Data-protection rules have also been addressed in many countries around the world. Over 100 countries now have data-protection laws in place, with the fastest growth seen in African countries. The EU's General Regulation on Data Protection (GDPR) unifies data privacy laws across Europe while protecting and empowering EU citizens' data privacy. GDPR provides a framework and serves as an example for many countries, albeit in the appropriate context and adapted to national realities, with Brazil, for example, adopting LGPD, and the State of California adopting CCPA. Other countries, such as Canada, Australia and India, are also considering legal and regulatory frameworks on personal data protection.

Starting in January 2012, three key pieces of legislation were adopted in the EU: a General Regulation on Data Protection (GDPR), adopted on 24 May 2016, applicable as of 25 May 2018;⁴ a specific Directive on data protection in the area of police and justice, adopted on 5 May 2016

¹ Centre on Regulation in Europe (CERRE). Event report. [Takeaways from the CERRE Executive Seminar. CERRE Executive Seminar on interpreting and implementing the new Electronic Communications Code](#). 22 January 2019.

² European Union (EU). EUR-Lex. [Directive \(EU\) 2018/1972](#) of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. 17 December 2018.

³ ITU-D SG1 Document [SG1RGQ/151 from India](#)

⁴ EU. EUR-Lex. [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 4 May 2016.

and applicable as of 6 May 2018;⁵ and Regulation (EU) 2018/1725 with regard to the processing of personal data by the Union's institutions, bodies, offices and agencies.^{6,7}

In addition to data protection, the E-Privacy Directive 2002/58/EC⁸ provides additional data-protection rules for telecommunication networks and Internet services and is currently under discussion in the European Parliament and the Council of the European Union. This new regulation should cover issues that arise from a rapidly evolving technological landscape, such as IoT or M2M.

1.2 Institutional reforms at international level, international organizations and associations, and global and regional cooperation: What is their role in consumer protection, and what are some of the new developments?

Many elements and stakeholders make up the digital economy and digital ecosystem. Consumer-protection principles and policies, as well as recommendations and standards adopted at the international and regional level, can guide policy-makers and regulators at the national level, especially in an increasingly interconnected world.

A discussion paper for the 2019 ITU Global Symposium for Regulators (GSR-19) defines stakeholders involved in consumer protection as follows:⁹

International stakeholders: The following international stakeholders are all involved with consumer protection: Organisation for Economic Development and Co-operation (OECD), United Nations, ITU, New Economics Foundation (NEF), World Bank (WB), Consumers International (CI), regional regulators associations (RRAs) and the International Ombudsman Association (IOA). The International Competition Network (ICN) aims to facilitate effective international cooperation for the benefit of member agencies, consumers and economies worldwide.

Regional stakeholders: By way of example, regional bodies having detailed consumer-protection recommendations or directives include:

- i. Association of Southeast Asian Nations (ASEAN)
- ii. Organization of American States (OAS)
- iii. European Union (EU) and European Commission (EC), and Body of European Regulators for Electronic Communications (BEREC)

⁵ EU. EUR-Lex. [Directive \(EU\) 2016/680](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

⁶ EU. EUR-Lex. [Regulation \(EU\) 2018/1725](#) of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

⁷ For an exhaustive overview of EU data-protection legislation, see also: European Union. European Data Protection Supervisor. [Legislation](#).

⁸ EU. EUR-Lex. [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

⁹ ITU. Global Symposium for Regulators (GSR). GSR-19 Discussion Paper. [Building confidence in a data-driven economy by assuring consumer redress](#).

- iv. European Consumer Organization (BEUC) (*Bureau Européen des Unions de Consommateurs*)
- v. African Union of Consumers
- vi. Pan-African Forum on Consumer Protection.

Recognizing that digital innovation and competition among digital service providers has improved consumer empowerment but remains complex, the 2021-2025 strategic plan of BEREC, for example, highlights the need to engage consumers in the fast-evolving digital ecosystem, and underlines the important role regulators play in ensuring consumer transparency and digital skills. The strategy states that BEREC seeks to promote choice and empowerment for end users by prioritizing work to build trust in ICT and digital services, and to enable consumers to make better informed choices.¹⁰

BEREC's approach to empowering end users is based on two pillars: The first relates to monitoring of the sector by including new end-user provisions, such as information on the contract summary template and inputs to the EC regarding the review of end-user rights. The second pillar relates to transparency, where BEREC will continue its work towards greater involvement of stakeholders, including consumer representatives, and publish its work in compliance with the BEREC regulation. As part of its work on transparency, BEREC will also build its knowledge base on artificial intelligence (AI) and explore ways to safeguard consumers against potential risks.

Advocacy groups, such as Consumers International,¹¹ have also illustrated ways and shared examples on how to protect consumers from security and other threats during the pandemic. The International Consumer Protection Enforcement Network (ICPEN)¹² has developed social media campaigns to promote consumer reporting of COVID-19-related consumer-protection issues.

The unprecedented COVID-19 crisis has accelerated the digitalization of many businesses and services, including teleworking and videoconferencing systems in and out of the workplace, access to healthcare, education and essential goods and services. The COVID-19 response has shown an increased need for inter-agency, regional and international cooperation. ITU's REG4COVID Platform¹³ illustrates examples of cooperation with competition or between communication regulators and consumer agencies to protect consumers from excessive communication service charges or price gouging.

1.3 Institutional reforms at the national level among different countries relative to consumer protection. Role of national regulatory authorities and other relevant authorities in consumer protection

The digital economy is global and not limited to national borders. There are many international movements and transactions that bring consumer protection to a global level, meaning that international coordination is essential. International principles are seen to be necessary, one example is being the 2016 UN Guidelines for Consumer Protection for online and offline

¹⁰ Body of European Regulators for Electronic Communications (BEREC). [BEREC strategy 2021-2025](#). Document BoR (20) 43. 5 March 2020.

¹¹ Consumers International. [Who we are](#).

¹² International Consumer Protection Enforcement Network (ICPEN). [Protecting consumers worldwide](#).

¹³ ITU. REG4COVID. [Global Network Resiliency Platform](#) (#REG4COVID).

commercial activities and dispute resolution and redress.¹⁴ Digital has brought new challenges and opportunities for consumer protection, including issues relating to e-commerce, data protection, spam and fraud.

As highlighted in the GSR-19 discussion paper already referred to, all consumers and providers of products and services are stakeholders in consumer protection. The paper identifies organizations which have a responsibility for oversight or advice on consumer protection at the national level, including:

- i. Governments
- ii. NRAs for regulated sectors and their advisory groups
- iii. Ombudsmen for different sectors
- iv. Competition authorities
- v. Consumer authorities
- vi. National citizen advice associations and local consumer champions
- vii. Consumer, industry and cross-sector forums
- viii. Courts providing judicial redress.¹⁵

The GSR discussion paper also identifies examples of national consumer-protection mechanisms:

- i. In **New Zealand**, the remit of the Commerce Commission includes oversight and regulation of the telecommunication/ICT sector. Other organizations which assist consumers in telecommunication/ICT/Internet-related issues include:
 - a. Telecommunications Dispute Resolution (TDR) to assist consumers in resolving complaints about landline, mobile and Internet issues. TDR was established by the Telecommunications Forum (TCF) and is consumer-led.
 - b. Citizens Advice Bureau (CAB) assists consumers on how to resolve complaints with a provider. If a complaint is not resolved, it is referred to TDR.
 - c. Ministry of Business, Innovation and Employment – Consumer Protection website provides guidance to consumers on such matters as how to complain about a faulty product or service and identifying, avoiding and reporting online scams.
- ii. In **Singapore**, examples include:
 - a. Infocomm Media Development Authority (IMDA) is the NRA and the statutory board in the Singapore Government responsible for regulating the converged infocommunication media sector, safeguarding the interests of consumers, and fostering pro-enterprise regulations and data protection through its Personal Data Protection Commission.
 - b. Consumer Association of Singapore (CASE) is a non-profit, non-governmental organization responsible for protecting consumers' interest through information, education and promoting an environment of fair and ethical trade practices.
 - c. The Competition and Consumer Commission of Singapore (CCCS) is responsible for administering and enforcing the Competition Act, administering the Consumer Protection Act, investigating and enforcing actions against practices that have an

¹⁴ United Nations Conference on Trade and Development (UNCTAD). [United Nations Guidelines for Consumer Protection](#). New York and Geneva, 2016.

¹⁵ ITU. Global Symposium for Regulators (GSR). GSR-19 Discussion Paper. [Building confidence in a data-driven economy by assuring consumer redress](#).

adverse effect on competition, representing Singapore in respect of competition matters in the international arena, and having a statutory duty to advise the government or other public authority on national needs and policies in respect of competition matters generally.

- iii. In the **United Kingdom**, Ofcom is responsible for media, telecommunications, post and ICT and has authorized:
 - a. Ombudsman services to deal with communication and media disputes. They work with trade bodies in the communications sector, including UK Wireless Internet Service Providers Association (WiSPA), Internet Service Providers Association (ISPA) and Internet Telephony Service Providers Association (ITSPA). The services are free to consumers as required by the Communications Act 2003. In the case of the Ombudsman services, funding is covered by the fee paid by the companies signed up to the Alternative Dispute Resolution (ADR) scheme. Ofcom sets out guidance for consumers on how to make a complaint to their communications providers.
 - b. The Centre for Effective Dispute Resolution (CEDR), which manages a communications and Internet service adjudication scheme (CISAS), is supervised independently by an ADR Provider.
 - c. Citizens Advice (CA) is a charity which assists consumers and small businesses with issues and to find a way forward. Their 'one service strategy' states that "Research clearly shows that people increasingly want and expect to get advice in person, on the phone, and through a range of digital devices - and to have a seamless experience. They want friendly, simple, intuitive services." CA provides independent consumer advocacy lobbying government policy-makers and regulators of essential services. They are lobbying to be the independent advocate for telecommunications.
- iv. In **Australia**, the Australian Communications and Media Authority (ACMA) has an established Consumer Consultative Forum (CCF), which is its main telco consumer advisory group. It brings together key stakeholders, including consumer organizations, the telco industry and government to raise and discuss important issues affecting users of telecommunication services, mobiles, Internet and fixed-line telephones. ACMA also works with the independent Australian Communications Consumer Action Network (ACCAN), a communications consumer organization representing individuals, small businesses and not-for-profit groups as consumers of communications products and services. ACCAN focuses on goods and services encompassed by the converged areas of telecommunications, broadcasting, the Internet and online services, including both current and emerging technologies.
- v. In **South Africa**, the Independent Communications Authority of South Africa (ICASA) is the regulator of the South African communications, broadcasting and postal services sectors. ICASA has a Consumer Advisory Panel (CAP) comprising 11 members who are nominated through a public process, including representatives of persons with disabilities, women, youth, senior citizens and people living in under-served areas with regard to ICTs.
- vi. In the **Netherlands**, in response to the COVID-19 crisis, a platform was created to support consumers. The Authority for Consumers and Markets (ACM) follows economic developments closely and will answer questions from consumers about their rights and from companies on cooperation to combat the crisis. ACM ConsuWijzer contains information for consumers, for example about cancelling trips, vouchers that companies now offer for products or services, or subscriptions that cannot continue. There are also tools for companies on the website.¹⁶

¹⁶ Ibid.

1.3.1 National monitoring, evaluation and enforcement mechanisms: Effectiveness of such measures - What can NRAs do? How to cooperate with industry? Which other players should be considered?

Current progress around the world shows that many, if not all, countries across the world have general consumer laws in place. However, the law is generally slow in catching up with the ever-changing bouquet of technological changes, which has resulted in products that did not exist or were not envisaged when the laws were promulgated. The main concerns in the new digital world include fraud, protection of privacy, prevention of unauthorized disclosure and unfair consumer contracts and billing procedures.¹⁷ Moreover, there have been efforts around the world to modernize telecommunication laws to cover AI and IoT. Guidelines and ethics related to data protection, privacy and transparency, autonomous vehicles and autonomous weapons are still emerging.

Due to drastic changes in the telecommunication/ICT sector, NRAs and policy-makers are reviewing their current regulations and policies regularly in order to facilitate technological improvements and adapt to the new digital environment. A contribution from **Zimbabwe** indicates that the COVID-19 pandemic has shown how regulators and policy-makers need to go back to the drawing board and come up with policies that encourage investment in rural and remote areas, especially for last-mile connectivity. It suggests that solutions connecting individual homes have become a priority for rural and remote areas.¹⁸

The National ICT Authority of **Papua New Guinea** (NICTA) is currently seeking to establish a performance measurement and monitoring regime with respect to retail telecommunication services. NICTA envisages that this information, when presented in a meaningful format, will enable consumers to better understand and compare the quality of services between different providers.¹⁹ Moreover, the primary focus of the Consumer Protection Rule that came into effect on 25 July 2014 is to encourage customer involvement, empowerment and confidence²⁰.

On 4 July 2019, the Government of **Burkina Faso** adopted the Digital Planning Roadmap of Burkina Faso. This roadmap will help reduce the country's digital divide in terms of access to high-speed and very high-speed broadband by 2030. In order to guarantee the roadmap's implementation, its strategy will comprise an institutional and organizational framework to promote coordination with the private sector and other countries in the region.²¹

In the **Democratic Republic of the Congo**, the aim of the reform of the legal framework, dating from 2002, is to make it possible to open up considerable market opportunities, secure investment and, in the longer term, ensure the development of a genuine digital society through the deployment of the national broadband backbone.²²

In the **Comoros**, in order to achieve an enhanced regulatory framework, draft laws are under consideration and planned to be brought before the National Assembly. The intention is to speed up the implementation of e-governance projects with a view to developing a digital

¹⁷ ITU-D SG1 Document [1/336](#) from Zimbabwe

¹⁸ ITU-D SG1 Document [SG1RGO/326](#) from Zimbabwe

¹⁹ ITU-D SG1 Document [1/329](#) from Papua New Guinea

²⁰ ITU-D SG1 Document [1/111](#) from Papua New Guinea

²¹ ITU-D SG1 Document [SG1RGO/178](#) from Burkina Faso

²² ITU-D SG1 Document [SG1RGO/171](#) from the Democratic Republic of the Congo

governance policy and creating an “e-Academy”, as well as improving coverage of white spots with the aid of a universal service fund.²³

In **Guinea**, massive use of the Internet has increased the risk of fraud. To regulate these abuses, the Guinean State adopted legal devices in 2016, in particular a law relating to cybersecurity and the protection of personal data, and a law relating to electronic transactions. A commission is being created for the protection of personal data.²⁴

Some of the measures that the **Central African Republic’s** Regulator has taken for the protection of consumer rights with respect to Law No. 18.002 of 17 January 2018 are as follows:²⁵

- Creating a consumer service within the new organizational structure of the Regulatory Authority for Electronic Communications and Posts (ARCEP)
- Creating an online space for consumers, called the Consumer Space, on the ARCEP website
- Producing brochures on the rights and obligations of consumers
- Establishing a partnership agreement between consumer associations and ARCEP.

The tools and procedures put in place by the **Benin** electronic communications regulatory authority to strengthen its role in institutional mediation aims, in particular, to reveal how regulatory authorities can become real mediation bodies for consumer protection in Africa. While settling disputes between consumers and operators, it is up to the regulatory authorities to choose the means by which they could arrive at an amicable settlement of disputes effectively and efficiently and in accordance with the requirements of the law.²⁶

In **China**, the Ministry of Industry and Information Technology (MIIT) and local communication-management agencies have formed a top-down regulatory system. In response to user concerns about personal information protection, unsatisfactory information governance and poor standards of service behaviour in telecommunication enterprises, MIIT has issued some policies to stipulate the rules for the use of personal information. MIIT has established a user complaint acceptance platform as well as a telecommunication user complaint acceptance agency. Third-party organizations, such as the National Telecommunications User Committee, China Communications Enterprise Association and the China Internet Association, participate in the formulation of laws and regulations, cooperate with supervision and inspection, accept consumer complaints and investigate infringement disputes.²⁷

In **Zimbabwe**, the work to come up with a consolidated piece of legislation has been going on for more than five years, and the Bill has now been presented to the Parliamentary Portfolio Committee for industry and commerce in preparation for Parliamentary approval. The Bill seeks to:²⁸

- Protect the consumers of goods and services by establishing a consumer-protection agency
- Regulate consumer advocacy organizations
- Repeal outdated laws, such as the Consumer Contracts Act.

²³ ITU-D SG1 Document [SG1RGO/170](#) from the Comoros

²⁴ ITU-D SG1 Document [SG1RGO/TD/5](#) from Guinea

²⁵ ITU-D SG1 Document [1/154](#) from the Central African Republic

²⁶ ITU-D SG1 Document [1/179](#) from Benin

²⁷ ITU-D SG1 Document [1/220](#) from China

²⁸ ITU-D SG1 Document [1/248](#) from Zimbabwe

In **Benin**, following several complaints to the Regulatory Authority for Electronic Communications and Posts (ARCEP) expressing opposition to the installation of radio stations, the Digital Code of the Republic of Benin was brought into force.²⁹ The aim was to facilitate the installation of radio facilities in conditions that take into account the protection of the public against non-ionizing radiation while safeguarding the environment.

Zimbabwe has made an effort to harness the innovative minds of young people and to further the development of ICTs in the country by implementing an innovation programme. The expected outcomes of the programme include the creation of home-grown solutions that improve the economic and social lives of Zimbabweans.³⁰

In **Haiti**, the administration set up a unit to follow up with operators in order to protect the rights of consumers to a quality of service in accordance with the operators' terms of reference and, on occasion, in relation to lost minutes and unsolicited advertising.³¹

The National Telecommunications Agency (Anatel) in **Brazil** ensures that it keeps Brazilians connected, even in times like the current pandemic. The agency monitors the measures developed by the service providers and discusses with them as well as with other bodies, local governments and civil society to find solutions that will address the legitimate concerns of all.³²

1.3.2 Capacity building: Digital skills and competency for regulators

One of the main barriers to greater uptake in an increasingly digital world is the lack of skills required to use digital products, services and content. Similarly, digital skills and competency among regulators must also evolve in order to adapt and adjust policies in a rapidly changing technological environment. Regulators should follow new technological advancements, take the lead in digital literacy, educate consumers and increase awareness, while providing a secure ICT environment that would ensure privacy for consumers. Every day, the competency of regulators becomes more vital for the development of their country. For this reason, regulators should find the best ways to increase their capacity in order to react to ICT developments in a timely manner and ensure consumers benefit from every new development in the ICT environment. There are many different initiatives related to increasing digital skills in a society that eventually affect the capacity and competency of regulators.

ITU recently launched the *Digital Skills Assessment Guidebook*, a comprehensive and practical step-by-step tool for national digital skills assessments.³³ The guidebook helps Member States to determine the existing national supply of digital skills, to assess skills demand from industry and other sectors, to identify skills gaps and to develop policies and address future digital skills requirements.

The ITU and World Bank *Digital Regulation Handbook* is a valuable and comprehensive resource to guide regulators in coping with the demands of the digital era. It emphasizes that "regulatory frameworks [for] the digital economy must not merely extrapolate present – and possibly outdated – laws and regulations to new players or new topics. Instead, policy-makers should adopt measures – which may include deregulation, self-regulation, or a co-regulatory approach

²⁹ ITU-D SG1 Document [SG1RGQ/169](#) from Benin

³⁰ ITU-D SG1 Document [SG1RGQ/241](#) from Zimbabwe

³¹ ITU-D SG1 Document [SG1RGQ/143](#) from Haiti

³² ITU-D SG1 [Document SG1RGQ/360](#) from Brazil

³³ ITU. ITU Academy. [Digital Skills Assessment Guidebook](#). Geneva, 2020.

- that will lead to greater innovation, easier deployment of new and emerging technologies, incentivize investment, and focus on inclusivity and collaboration".³⁴

The diffusion of ICT in the workplace is not only raising the demand for ICT specialist and generic skills, it is also changing the way work is carried out and increasing the demand for ICT complementary skills. These are skills that are not related to the capability of using the technology effectively, but rather to carrying out the work within the new environment shaped by ICTs - in effect a technology-rich environment. While there is general awareness that education curricula must evolve to adjust to these changes, little is known about the type of skills that should become more important in the curricula.³⁵ The Digital Regulation Handbook affirms that "the ICT regulator's role includes supporting grass roots and regional or national consumer groups to get organized, to support individuals with problems and gather consumers' views on digital issues [and] engaging with those groups, both to help with their consumer education and to learn from them how well current policies are working".³⁶

In the EU, The European *Digital Competence Framework*, also known as DigComp, offers a tool to improve citizens' digital competence. Today, being digitally competent means that people need to have competences in all areas of DigComp. The eight proficiency levels (using a metaphor of "Learning to swim in the digital ocean") and examples of use can be found in DigComp 2.1.³⁷ The Digital Competence Framework can help monitor citizens' digital skills and to support curricula development.

Regulators should monitor their digital competence levels and update education and training activities regularly. For example, AI could be expected, as with ICTs more generally, to enhance the need for new skills, such as programming and developing AI applications or being able to leverage AI.³⁸

1.3.3 Awareness-raising mechanisms that can be used by policy-makers and regulators (campaigns, services, etc.)

Telecommunication regulations are increasingly focused on measures to be taken to increase awareness among consumers and promote consumer-protection rules. In order to guard consumers against deceptive practices and to empower them with practical tools to resolve their problems, such awareness-raising mechanisms have gained vital importance. Likewise, new consumer-protection frameworks should be adopted in the converging environment.

The concept of consumer satisfaction mostly assumes that consumers have enough knowledge about their products and services as well as their expectations about them in order to make decisions in their best interest. However, it is argued that consumers may either not report their complaint or simply change operator, due to biases such as maintaining the status quo.

On the other hand, in the digital environment, standard business-to-consumer contracts are generally used to fulfil an efficiency role in the mass distribution of goods and services. These contracts have the ability to trick or abuse consumers because of the unequal bargaining power between the parties. Typically, the consumer is in no position to negotiate and to alter the

³⁴ ITU-D SG1 Document [SG1RGO/373](#) from the BDT Focal Points for Questions 1/1, 3/1, 4/1 and 6/1.

³⁵ Organisation for Economic Co-operation and Development (OECD). OECD iLibrary. [OECD Digital Economy Outlook 2017](#). Paris, 2017.

³⁶ ITU-D SG1 Document [SG1RGO/373](#) from the BDT Focal Points for Questions 1/1, 3/1, 4/1 and 6/1.

³⁷ EU. EU Science Hub. [DigComp - European Digital Competence Framework](#).

³⁸ OECD. OECD iLibrary. [OECD Digital Economy Outlook 2017](#). Paris, 2017.

standard terms. If there is time to read them, it is doubtful whether the purchaser will understand the meaning and impact of each term in the light of the whole contract.

These new market structures make consumer awareness more important. In order to achieve a healthier digital ecosystem in an era of rapid technological progress in the ICT industry, consumers need to understand the limits of consumer power and recognize attempts at misleading or manipulating them. They must also be aware of the emergence of monopolies or dominant market players locking consumers into certain consumption patterns by restricting consumer choices.

The Federal Telecommunications Institute (IFT) of **Mexico**, the regulatory body for telecommunications in the country, has launched the *Digital Alphabetization Programme*. Through learning courses, talks and informational stands, this programme helps empower users to know and identify their rights as users of telecommunication services and the way to make them enforceable. This initiative promotes the use of digital tools which IFT has developed, such as the 'Comparator of Telecommunication Services', 'Mobile Coverage Maps', 'Calculator of Probabilities of ICT Use', and 'I am a User', among others.³⁹

In order to help consumers decide optimally, regulators should find ways to empower consumers and increase consumer education and awareness, such as of available options of products and services. This way, in the event that a consumer faces a violation, they may be aware of their rights and report the matter to the responsible authorities. Moreover, since increasing consumer awareness is becoming more and more important every day because of the use of standardized contracts, governments need to review their consumer-protection policies, and regulators may need to introduce adequate regulations to increase consumer awareness so they can benefit from the advancement of ICTs.

1.3.4 Looking to the future: Collaborative regulation between policy-makers and regulators, between different regulators, between regulators and industry, and between regulators and consumer associations, both within the ICT sector and across other sectors

As ICTs have taken their place at the centre of every economic sector, collaboration has become vital to harmonize policy and regulatory frameworks that have evolved independently in many sectors over the years. Shared perspectives and common responsibility and a robust balance between people's rights and the technology that impacts so much on our everyday lives call for collaborative regulation in order to fast-forward digital transformation for all. Such collaboration must bring together a broad and diverse range of stakeholders when making rules or decisions, keeping in mind its social and economic impact.

ICT regulators and policy-makers play a leadership role in order to connect peers across all economic sectors to facilitate digital transformation. They need to follow a cross-sectoral, open and highly collaborative regulatory approach and try to afford adequate protection to consumers.

ITU has defined the notion of collaborative regulation (fifth generation regulation) in order to assist regulators and policy-makers. This '5th generation regulation' offers a framework for discussing the evolution of regulatory patterns and policies towards digital transformation,

³⁹ ITU-D SG1 Document [1/349](#) from Mexico

while charting the way ahead for industry and regulators as one constituency. With the goal of bringing together all stakeholders – from policy-makers and single-sector and cross-sector regulators to market players of any size – 5th generation regulation marks a fundamental shift in the way regulation is executed in a holistic, cross-sectoral context.

The Global ICT Regulatory Outlook 2020 report has also featured a new tool, the *Benchmark of Fifth Generation Collaborative Regulation*, with the aim of creating a Gold Standard for collaboration among regulators. In order to take full advantage of digital transformation, the G5 Benchmark enables stakeholders to fast-track collaborative and cross-sector regulation. It provides metrics to assess gaps, proposes roadmaps through shifting regulatory landscapes, and tracks progress. The aim of the G5 Benchmark is to offer a big-picture, higher-level view enabling regulators not only to see the landscape clearly laid out below them, but also their routes across it to G5 regulation.⁴⁰

According to the G5 Benchmark, there are four fundamentals for better progress towards collaborative regulation:

- ICTs have moved far beyond the realm of simple communications. They have become the foundation for every economic sector and an essential condition for business performance and national growth.
- ICTs can dramatically transform education, healthcare, environmental management, agriculture, trade and entrepreneurship, government services... and so much more. In order to achieve this, enabling frameworks of policy and regulation need to be put in place along with the right networks and services.
- Silo-style ICT-sector regulation is not viable in the digital world. Collaborative regulation will mirror the interplay between digital infrastructure, services and content across industries and national borders. It will also harmonize rules and ensure consistent implementation of policy and regulatory frameworks that have evolved independently in many sectors over the years.
- Collaborative regulation is people-centred regulation. It looks at sustainability and long-term gains as opposed to industry profit maximization and exclusive economic growth (connecting marginalized individuals, persons with disabilities, low-income communities, communities challenged by educational impoverishment, and remote or isolated populations that may also lack basic infrastructure such as electricity).

In conclusion, since the traditional telecommunication market is transforming into a new complex digital world, where bundling of products and services from different markets is becoming the norm, this new digital world requires NRAs to collaborate closely with other authorities, such as consumer-protection institutions, data-protection agencies, competition authorities and all other relevant organizations within the country in order to cover all new digital and innovative services. It is essential to work together with other authorities to protect consumer rights in a market where boundaries are blurring. For example, as Internet service providers (ISPs) increasingly offer joint services with content providers, safeguarding fair competition not only within telecommunication markets but also across adjacent markets becomes more essential. This concern requires NRAs to cooperate with competition authorities. Likewise, since consumers are more concerned with privacy in this new digital environment compared to that of traditional telecommunication services, collaboration with data-protection agencies becomes more vital to alleviate the privacy concerns of consumers.

⁴⁰ ITU. Studies & research. [Global ICT Regulatory Outlook 2020: Pointing the way forward to collaborative regulation](#). Geneva, 2020.

Chapter 2 – Consumer evolution: New challenges in a digital world

2.1 Introduction

Digital communications have brought the world closer in many ways. Near seamless cross-border digital communications have touched almost every aspect of human existence, revolutionizing economic activity, bringing useful services to consumers, facilitating the exchange of information and ideas, and improving lives in unprecedented ways. At the same time, as more and more people and activities move online, there have been growing concerns about many consumer-protection issues, including safety, security, competition and consumer rights. This has brought forth a variety of regulatory responses in different jurisdictions. However, a fragmented approach towards regulation could be detrimental to both continued growth and innovation in this important area. Digital communications-based technologies cut across economic activity and transcend national boundaries, necessitating a re-think of present institutional arrangements to regulate online activities and protect consumers.

It is quite clear that there are novel challenges in digital regulation today, which will require innovative technological measures and fresh regulatory approaches. Tackling these challenges entails collaboration among sector regulators and the active cooperation of technology companies. The latter must come forward with better self-regulation and technological solutions to prevent potential harm from online activities.

Across the world, governments generally work in the best interests of their citizens and economies, attempting to balance measures to protect consumer privacy, secure data and ensure safety in digital communications with the need to safeguard continued innovation and competition. While respecting the jurisdiction of Member States, ensuring the continued benefits of the digital revolution requires that regulators and policy-makers across the world cooperate and coordinate their efforts. This is necessary because of the cross-border nature of online activities and their global impact. There is thus an urgent need for international collaboration and capacity building on various aspects of digital regulation.

Such an approach would help create an effective system of regulation that:

1. Ensures consumer protection, and thereby sustains consumer trust in the use of digital communications services
2. Does not create conflicting compliance requirements.

Both these conditions need to be met to avoid hampering the pace of innovation and consumer benefits that accrue from the unique, innovation-driven opportunities presented by digital technologies.⁴¹

⁴¹ ITU-D SG1 Document [SG1RGQ/151 from India](#)

2.2 New business models (infrastructure, content and applications)

There are many ways of looking at digital convergence, but it is generally acknowledged to be the result of the shift towards IP-based networks combined with the proliferation of high-speed broadband access and multimedia communication and computing devices. It presents huge opportunities for application and service providers to serve consumers better. It has led to the emergence of new business models that have taken advantage of innovations that do not necessarily fall in the ambit of present regulatory frameworks and are independent of the network service provider. An OECD paper on convergence explains that the synergy between 'network, applications and new devices' has given rise to the phenomenon of a 'new value chain' by way of 'platformization' wherein service providers functioning at different levels of digital communication networks leverage their "specific assets" (for example, content, networks and search engines) to serve a variety of consumers and markets.⁴² The change in business models takes place not only in the realm of digital communications *per se* but across the economy. Thus, firstly, wireless services have either complemented or replaced fixed-line services. Secondly, over-the-top services (OTTs), or apps like WhatsApp and Skype, compete with traditional voice and SMS. Thirdly, OTTs, like Uber and Airbnb, compete with bricks-and-mortar businesses. The changes also take place at the device end, where the mobile handset becomes a converged device which can home in on a variety of networks, such as Wi-Fi, mobile and Bluetooth, and deliver a host of services. New communication technologies like 5G will facilitate greater use of IoT/M2M communications in health, education, agriculture, smart cities and manufacturing and will further disrupt markets and create new business models that will affect both the manner in which underlying digital communication networks are configured and also how services are delivered across economic sectors.

ICT service providers are consequently able to switch from being simple suppliers of connectivity to providers of more than one service. With innovations in information technology, there are more and more kinds of information products. Interactive, intelligent networking hardware has become a new direction of information products. Telecommunication operators take "IPTV + OTT + Home Service" as the starting point to gradually improve the smart-home product chain, such as intelligent gateway, smart speaker, smart-home app and so on. The application scenario of personal information consumption has changed from fragmentary to full coverage of clothing, food, housing and transportation. The convergence business of mobile payment, instant messaging, e-commerce, video and video applications has developed rapidly.⁴³

All this gives rise to new challenges in terms of regulation for consumer protection and in terms of compliance for service providers as well. For example, the cloud is the new ICT paradigm that gives an impressive acceleration to the digital explosion based on data usage and manipulation, imposing contemporarily a strict observance of the increasingly incumbent rules issued to safeguard privacy and data protection. Our dynamic use of the Internet through computers and mobile devices provides many businesses with the capability to collect a plethora of information about our private lives, movements, locations, preferences and lifestyles. This has enabled a revolution in marketing methodologies and tools that provide extraordinary insight into customer needs and opportunities. Therefore, a clear definition of guidelines aimed at guaranteeing the compliance of every cloud application with the data-protection regulations is

⁴² OECD. OECD iLibrary. OECD Digital Economy Papers. [Digital Convergence and Beyond: Innovation, Investment and Competition in Communication Policy and Regulation for the 21st Century](#). 7 June 2016.

⁴³ ITU-D SG1 Document [1/220](#) from China

required.⁴⁴ For providers of cloud services, compliance challenges exist, and a variety of different regulatory approaches would make providing cross-border services very difficult.

2.3 The changing requirements of consumer protection in era of converged services

In the digital age, the nature of ICT services is changing and evolving. The number of consumers of telecommunication and IT services is increasing significantly as a result of the launch of many new services. According to ITU, in 2018 nearly half the world's population – more than 3.4 billion people – owned smartphones, and there were more than 4.2 billion active mobile-broadband subscriptions worldwide at the end of 2017.⁴⁵

A contribution from China has highlighted that in recent years, China's information consumption has developed rapidly. The consumption capacity of residents improved greatly, and the scope of consumption has also expanded, integrating innovation and cross-industry convergence. The support capacity of networks has been continuously enhanced, which has become one of the most important engines to promote China's economic development. Meanwhile, the expansion of information consumption continues and consumer groups have become increasingly diverse, which raises new requirements and challenges for the protection of consumer rights and interests. Applications that drive the explosive growth of mobile Internet access traffic, live broadcasting, short videos, games, children's education and others have stimulated the rapid growth of data consumption, and residents' expenditure on communication services has gradually shifted from traditional voice services to data services.

The nature of consumer protection in the area of converged services has consequently changed and will continue to do so because of rapid technological evolution, the emergence of new services and their widespread uptake. Today, the Internet as we know it is the sum of multiple networks running on various media and owned by different entities. It provides us with a range of services and applications that cut across the economy. Converged services in the digital economy cover – but are not limited to – communications, Internet, OTT services, media, content, digital financial services (DFS) and e-commerce.⁴⁶ The situation is characterized by 'pervasiveness, technological dynamism, and general productivity gains'.⁴⁷ While consumer protection traditionally focused on public safety, fair and reasonable contract terms and the protection of vulnerable consumers, in view of the emergence of new applications and business models as described above the existing consumer-protection framework may no longer be sufficient. This is especially so as new challenges in the area of privacy, data security and competition have emerged.

Regulatory response can no longer be symmetric in the sense that given the vast variety of services and applications there can be no one-size-fits-all solution. Regulators need to exercise caution so as to avoid hindering innovation and growth of digital services. Yet, consumer safety and trust are equally important issues to be addressed if the pace of growth is to be sustained. Further, regulation of online services and content will have to factor in the cross-border nature

⁴⁴ ITU-D SG1 Document [SG1RGQ/35 from Proge Software \(Italy\)](#)

⁴⁵ ITU. Thematic reports. Regulatory & market environment. [Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security](#). Geneva, 2018.

⁴⁶ ITU. Global Symposium for Regulators (GSR). GSR-19 Discussion Paper. [Building confidence in a data-driven economy by assuring consumer redress](#).

⁴⁷ OECD. OECD iLibrary. OECD Digital Economy Papers. [Digital Convergence and Beyond: Innovation, Investment and Competition in Communication Policy and Regulation for the 21st Century](#). 7 June 2016.

of new businesses, which complicates matters and raises jurisdictional issues in the regulation of consumer protection.

The GSR-19 discussion paper on *'Building confidence in a data-driven economy'* highlights the complexity of the digital economy and affirms that "it can only function through national governments adopting international standards to enable interoperability and international consumer protection principles and policies, recommendations and standards". It stresses the need for regulatory oversight by one or more NRAs, with common consumer-protection and redress regulations covering the converged services.

2.4 The main future challenges: Consumer trust and security

Policy-makers and regulators responsible for ICTs have played a significant role in bringing people online by creating a conducive environment, promoting investment and fostering the growth of high-speed connectivity, content, services, applications and other building blocks of the Internet. This has resulted in increasing competition among ISPs and platforms and stimulated growth of the digital economy.⁴⁸

The creation of a conducive environment through regulations and the necessary legislation will encourage greater investment in infrastructure and services. While recognizing the vast business potential of digital services, it is vital to assess whether the rights and interests of individuals are being adequately protected in this changing environment.⁴⁹Hence, the evolving needs of the ICT market and its success in providing business and services require greater efforts to protect consumers. The UN report entitled *'The Age of Digital Interdependence'*⁵⁰stresses that privacy implies a person's choice as to who can view or use personal information, while security is about protecting data on servers and networks. To ensure consumers' trust in digital services, both are needed as lack of security would encroach on privacy.

2.4.1 Privacy and consumer protection (digital identity, protection of personal data, privacy issues)

The phenomenal growth of digital services and the Internet has given birth to entirely new markets: those dealing in the collection, organization and processing of personal information, whether directly, or as a critical component of their business model. Identification has become very important to mobile connectivity. Digital identities facilitate digital, financial and even social inclusion. The collection and analysis of user data enable both businesses and governments to provide better services. At the same time, vast improvements in surveillance technology and the availability, storage and mining of personal information online, supported by developments in big-data analytics, have created a public-policy conundrum over balancing the benefits of big data with the threat to the right to privacy. This has become evident during the recent COVID-19 pandemic, during which many governments have used contact-tracing mobile apps (digital tools to map proximity between individuals, as a proxy for infection risk) to contain and reverse the spread of COVID-19. However, even in times of crisis this can be balanced with consumer rights. For example, EU Member States are converging towards effective app solutions that minimize the processing of personal data, and recognize that interoperability between

⁴⁸ ITU Document [SG1RGQ/153+Annex from the BDT Focal Point for Question 6/1](#)

⁴⁹ ITU-D SG1 Document [SG1RGQ/34 from India](#)

⁵⁰ United Nations. [The Age of Digital Interdependence](#). Report of the UN Secretary-General's High-level Panel on Digital Cooperation. June 2019

these apps can support public health authorities.⁵¹ EU Guidelines in this regard highlight the importance of applying principles, such as purpose limitation, proportionality, data minimization and transparency, to safeguard the privacy of consumers.⁵² Industry, too, has made efforts to proactively develop guidelines. One such example is the GSMA Guidelines on sharing mobile network operator data for contact tracing during the pandemic. These guidelines emphasize cooperation with governments as well as the importance of legality, anonymization, security and consumer privacy.⁵³

Thus, in an environment of pervasive surveillance and intrusive technology, there is a need for improved protection of privacy rights of consumers through a mixture of legislation and regulation as well as building public awareness and demanding safeguards. Regulating data is also important to ensure consumer safety and security, including protection from malware and cybercrime.

From a consumer-protection viewpoint, adopting data-protection laws and regulations to safeguard the interests of citizens is important as technological developments like M2M/IoTs, AI and 5G will entail the collection and harnessing of ever-increasing amounts of data. An OECD report has pointed out that data-gathering practices by platforms can heighten information asymmetry such that while the consumer is rendered transparent to the platform, the platform's practices remain opaque to the consumer.⁵⁴

The business case for focus on data protection also rests on building consumer trust in otherwise intrusive applications/use cases of new technologies. In the absence of trust in the security of these applications and technologies, we cannot expect new technologies to grow and flourish. For example, an UNCTAD note⁵⁵ on '*Strengthening consumer protection and competition in the digital economy*' has highlighted the sharply growing concern among consumers about online privacy. According to a 2019 survey on Internet security and trust, 78 per cent of those surveyed were concerned about online privacy, with over half (53 per cent) more concerned than one year previously. And, in economies in Africa and the Middle East, distrust with regard to e-commerce platforms had increased the most year-on-year (+9 points). Further, sustained growth depends on promoting competition by allowing the secure flow of data between entities (data portability rules) and across borders (issues of data security / localization). However, while regulating, care must be taken to also protect and sustain the competition and innovation that has yielded so many consumer benefits.

This has been recognized by ITU, as can be seen from the text below extracted from the 2017 *Buenos Aires Action Plan*:⁵⁶

⁵¹ ITU. REG4COVID. [EU launched toolbox for Mobile applications to support contact tracing in the EU's fight against COVID-19](#). 15 April 2020

⁵² [European Data Protection Board \(EDPB\). Guidelines. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak](#). 21 April 2020

⁵³ GSM Association (GSMA). Public Policy. [COVID-19 Privacy Guidelines](#). 6 April 2020.

⁵⁴ OECD. [Toolkit for protecting digital consumers: A resource for G20 policy-makers](#). OECD, 2018

⁵⁵ UNCTAD. [Strengthening consumer protection and competition in the digital economy](#). Note by the UNCTAD secretariat. *Eighth United Nations Conference to Review All Aspects of the Set of Multilaterally Agreed Equitable Principles and Rules for the Control of Restrictive Business Practices* (Geneva, 19-23 October 2020). Document TD/RBP/CONF.9/4 of 29 July 2020.

⁵⁶ ITU. Buenos Aires Action Plan. [Final Report of the World Telecommunication Development Conference \(Buenos Aires, 2017\) \(WTDC-17\)](#). Buenos Aires, Argentina, 9-20 October 2017. p. 693.

“Faced with the rapid evolution of technologies and the appearance on the market of ever more sophisticated equipment, consumers who are not telecommunication/information and communication technology (ICT) experts can find themselves at a loss. Consequently, consumer information and consumer rights have become a priority ... Given the pace of change in telecommunications/ICTs, bodies responsible for consumer protection (regulators, public and private agencies) should regularly amend their regulatory frameworks on the basis of the right balance between the interests of operators/service providers and those of users in areas such as subscription agreements, protection of intellectual property rights and management of digital rights, without detriment to innovative models of e-commerce...”

It is important to ensure that data-protection rights of individuals are being adequately protected in this changing environment. The data-protection regulator may not be able to intervene if consumer consent is given voluntarily. However, the question remains as to whether the consumer was well-informed and whether they had a real choice. Sector regulators could intervene in the event of a price/QoS/consumer-protection issue. To the extent privacy is a valued characteristic of a service transaction, excessive personal data collection in digital transactions can be seen as a QoS issue, and to the extent consumers pay for digital services with personal data, privacy can be equated with price, making big data a direct QoS/pricing issue associated with free online services in particular.

Digital players often provide free services. In the process they also acquire valuable personal data which is used for customized services and behavioural advertising. As long as the market is competitive and data use can yield innovations that benefit consumers, this may not be harmful. However, network effects and economies of scale and scope driven by big data can also confer market power and a durable competitive advantage. Market power can also lead to switching costs when customers may be compelled to use the (few) dominant service provider(s) despite privacy concerns (or annoying advertisements). As regulation catches up with technological change, regulatory gaps can be detrimental to consumer interests and competitive market conditions. It is thus imperative that regulators strive to understand, cooperate and coordinate so as to implement protective and corrective measures.⁵⁷A contribution from **India** describes India’s e-commerce regulation that aims to promote competition and protect consumers in online markets. It stresses that a combination of encouraging self-regulation by market players and filling gaps with State regulation is required to ensure consumer protection.⁵⁸

One such issue is differential pricing. Sellers can use big data and algorithmic processing of their personal data to target consumers with the right emotional pitch to increase overall consumption. Secondly, as more online retailers personalize pricing and product offerings, it will be harder for consumers to discover a general market price and assess their outside options, implying that behavioural discrimination becomes more durable. As consumers increasingly accept that prices change rapidly (such as airfares and hotels), they have lower expectations of price uniformity among competitors and would not be able to distinguish between dynamic and discriminatory pricing. Further, relying increasingly on intermediaries like search engines and digital assistants to search for products and services makes consumers extremely vulnerable to price discrimination based on personal characteristics. Yet this problem does not easily fall within the realm of either sector or competition regulators.

⁵⁷ ITU-D SG1 Document [1/198](#) from India

⁵⁸ ITU-D SG1 Document [1/344](#) from India

Across the world, privacy and data protection are receiving the attention of regulators. The **European Union** has put in place a comprehensive system through the GDPR,⁵⁹ which regulates the collection, processing and use of the data of consumers in the EU and is binding on all online traders when selling online to the EU market.⁶⁰ It has been widely emulated by other nations.

India has formulated a draft *Personal Data Protection Act*, which empowers consumers by acknowledging their right to privacy and affording them control over their personal data. This draft act is based on established principles, such as consent, purpose limitation, storage limitation and data minimization.

Brazil adopted legislation on personal data protection in 2018. Law N° 13.709 was approved on 14 August 2018, following a long period of discussion in the Brazilian Congress. This law was amended by Law N° 13.853, approved on 8 July 2019, and entered into force in February 2020. The law was strongly inspired by the European approach to personal data protection, although there are some differences. For instance, the Brazilian law establishes ten different legal grounds for processing personal data (while the GDPR has only six), including consent and the legitimate interests of the controller, among others. An interesting aspect is that Brazilian legislation applies to any processing operation carried out by any individual or by public or private entities (regardless of the country and where the data are stored, whether the data are collected in Brazil, or if the purpose of the processing activity is to offer or provide goods and services in Brazil, or to process data of individuals located in Brazil). An essential part of the law is, in fact, the creation of the National Data Protection Authority, a result of the amendment by Law N° 13.853. Many of the legal provisions will require interpretation and further regulation.⁶¹

After a two-year period, the Brazilian Personal Data Protection Law (*Lei Geral de Proteção de Dados Pessoais* - LGPD) (Law N° 13.709 of 14 August 2018) finally entered into force on 18 September 2020. The exceptions are Articles 52, 53 and 54. These articles refer to the enforcement of administrative sanctions and, as amended by Law N° 14.010 of 12 June 2020, will enter into force on 1 August 2021.

The National Data Protection Authority (*Autoridade Nacional de Proteção de Dados* - ANPD) had its structure approved by Presidential Decree N° 10.474 of 26 August 2020. The decree conditioned its entering into force on the publication, in the Union Official Gazette, of the appointment of the Director-President of the Authority, which happened on 6 November 2020, alongside the appointment of the other directors that compose the governing board of the Authority.

On 28 January 2021, ANDP published its regulatory agenda for 2021-2022.

China reports that it has achieved remarkable success in the protection of consumer rights and interests by establishing a government-led multistakeholder supervision and protection system. However, there is a constant need to continue following up on new problems brought about by the integration of the rights and interests of cross-industry users. As markets develop, industry supervision and protection systems need to be continuously improved in order to effectively

⁵⁹ EU. EUR-Lex. [Regulation \(EU\) 2016/679](#). (op. cit.)

⁶⁰ UNCTAD. [Strengthening consumer protection and competition in the digital economy](#). Note by the UNCTAD secretariat. (op. cit.)

⁶¹ ITU-D SG1 Document [SG1RGQ/215](#) from Brazil

protect the legitimate rights and interests of users.⁶²Further, according to the UNCTAD cyberlaw tracker, only 58 per cent of countries have privacy laws that apply to the online context.⁶³

2.4.2 Trust in security in the use of digital services

The evolution of ICTs has brought various benefits for economic and social development, but also various risks, such as the loss of information, phishing and fraud.

Inspiration can be taken from **Mexico**, where the Federal Telecommunications Institute (IFT), Mexico's telecommunications regulatory organ, carries out analyses and surveys to identify consumption patterns, levels of satisfaction and the user experience of telecommunication service users as well as promoting user interests, rights and behaviour when developing regulatory policies.⁶⁴It helps to monitor fixed and/or mobile Internet users' perception of cybersecurity and ascertain whether they had fallen prey to fraud, phishing or the misuse of personal data, and, if so, whether they knew whom to contact.

As highlighted by OECD, the misuse of personal data, regardless of whether it was accidental or deliberate, can cause significant harm in terms of distress and loss. The loss of reputation of an organization that undergoes a data breach can be serious for both the firm and for overall trust in the use of digital services. The impact on an organization experiencing a data breach, too, can be severe. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals alike. Good practices to counter loss of trust include the introduction of certification schemes, such as privacy certification.⁶⁵

As stated in an ITU study, privacy and cybersecurity must be an integral part of service offerings and innovation across the entire ICT industry. The ITU report in question also emphasizes the need for regulators to "understand the digital economy, technological advances, and the challenges facing both consumers and companies".⁶⁶Capacity building of consumers and regulators is important, as research indicates that newcomers to the Internet, such as populations in emerging economies like China and India, tend to trust digital services more than populations that have longer exposure to the Internet;⁶⁷this could put millions of people at risk even as they experience the benefits of digital connectivity.

The United Nations Report on digital cooperation suggests that governments engage actively with industry and civil society to discuss regulation, articulate values about technology development and usage, promote transparency about vulnerabilities and data breaches, and encourage genuine consent, privacy and security.

2.4.3 Ethics (address best practices in the public and private sectors as well as in new contexts such as AI)

IoT and AI are the most important new technologies that have the potential to make a significant difference in the daily lives of consumers. They enable communication between machines,

⁶² ITU-D SG1 Document [1/220](#) from China

⁶³ UNCTAD. [Strengthening consumer protection and competition in the digital economy](#). Note by the UNCTAD secretariat. (op. cit.)

⁶⁴ [ITU-D SG1 Document 1/194](#) from Mexico

⁶⁵ OECD. [Toolkit for protecting digital consumers: A resource for G20 policy-makers](#). OECD, 2018.

⁶⁶ ITU. Thematic reports. Regulatory & market environment. [Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security](#). Geneva, 2018.

⁶⁷ Ibid.

equipment and things in everyday use, replacing humans. The impact of IoT and AI cuts across many fields, such as health, education, logistics and agriculture, and makes Industry 4.0 a reality. These technologies are designed to have a positive impact on consumers' lives and facilitate their daily requirements. However, owing to their pervasiveness, a high level of security in applications and systems is needed to reassure consumers.

There is also the need for a discussion on the ethics involving new applications related to IoT and AI, including robotics, to ensure they will not adversely affect consumers' lives. Both regulators and service providers must focus on the incorporation of privacy and ethics by design and consumer awareness.

Handling these unique challenges requires appropriate institutional mechanisms within Member States that would keep abreast of latest technologies and advise on cross-sectoral legislation and regulation, including areas of consumer awareness and protection. There is also a need for international consensus and cooperation on standards, ethics and consumer protection. As with other consumer-protection issues in the digital age, those emanating from the use of AI will also require regulatory collaboration and capacity building at both the national and international levels. The ultimate aim is to harness the benefits of technology, while safeguarding against potential harm.

Among recommended best practices, governments should develop an AI national plan to outline key strategies to prepare for AI. One example is found in **India**, where the National Institute for Transforming India discussion paper entitled 'AI for All' lays the ground for the *National Strategy on Artificial Intelligence*.⁶⁸ It highlights the above-mentioned issues of privacy and security, including a lack of formal regulations around anonymization of data, among the barriers to adoption of AI. It recognizes that data is one of the primary drivers of AI solutions, and that appropriate handling of data while ensuring privacy and security is of prime importance. The challenges identified include data usage without consent, risk of identification of individuals through data, data selection bias and the resulting discrimination of AI models, and asymmetry in data aggregation. The paper suggests establishing appropriate data-protection frameworks and sectoral regulatory frameworks as well as the adoption of international standards.⁶⁹

2.5 Conclusion: Collaborative regulation, international cooperation and consumer education

Given the pace of change in telecommunications/ICTs, institutions and regulators responsible for consumer protection (regulators, public and private agencies) should regularly amend their regulatory frameworks based on striking the right balance between the interests of operators/service providers and of users in areas such as subscription agreements, protection of intellectual property rights and the management of digital rights, without affecting innovative models of e-commerce. One of the key challenges for regulators is to establish a culture of security that promotes trust in telecommunication/ICT applications and services, while effectively enforcing privacy and consumer protection. Therefore, it is essential to implement laws, policies and regulatory practices, and to develop transparent, effective consumer-protection mechanisms in order to build such trust and confidence.⁷⁰ As highlighted in the GSR-20 *Best-Practice Guidelines for Digital Regulators*, an adaptive, resilient, collaborative and fit-for-purpose

⁶⁸ Government of India. NITI Aayog. [National Strategy on Artificial Intelligence](#). June 2018

⁶⁹ ITU-D SG1 Document [1/307 from India](#)

⁷⁰ ITU-D SG1 Document [SG1RGQ/34 from India](#)

regulatory ecosystem is hence necessary for open and competitive digital markets to thrive along with delivering positive consumer outcomes and thus provide the foundation for Digital Transformation. The guidelines state that consumer interest and fairness are central to digital regulation, and all regulatory decisions should be taken with consumers in mind.⁷¹

Further, customers themselves should also be careful and take necessary precautions. They should carefully read the terms and conditions, install and update antivirus software, change passwords and back up information regularly, connect to secure public networks, and so forth.⁷² A critical aspect of consumer protection is digital literacy. Consumers themselves must be aware of their rights over their personal data and become mindful of security and privacy and other issues that may arise with the use of online communication. Regulators should strive to create such awareness among consumers. Child online protection is a significant facet of digital literacy. The GSR-19 discussion paper on *Building confidence in a data-driven economy* states that “the most powerful way of empowering and protecting consumers is through ensuring people are digitally literate, complemented by regulatory and legislative protection which has been influenced by strong consumer advocacy”.⁷³

While different models are evolving across the world, ultimately the appropriate regulatory design for consumer protection in the digital age would probably be a mix of government rules, industry self-regulation and co-regulation. Regardless, it is important for industry, regulators and academia to come together to achieve the stated objectives of data protection, privacy, competition and security so as to ensure, *inter alia*, the continued growth of digital services in a manner that benefits all stakeholders.

Further, developing an appropriate regulatory framework that will act as the foundation for good business practices and adequate consumer safeguards requires collaboration and international cooperation. The recent UN report on *Digital Cooperation - The Age of Digital Interdependence* highlights not only the need for shared standards but also the norms and values that should underlie digital cooperation - inclusiveness, respect, human-centredness, human-flourishing, transparency, collaboration, accessibility, sustainability and harmony. Furthermore, calling for greater harmonization, it has correctly pointed out that “taxation, trade, consumer protection and competition are among the areas of economic policy that require new thinking in the digital age; they are the ‘guard rails’ of the digital economy”.⁷⁴

Increased cooperation and capacity building could lead to effective national approaches and sharing of experience, thereby informing regional and global multilateral cooperation arrangements.⁷⁵

⁷¹ ITU-D SG1 Document [SG1RGQ/374](#) from the BDT Focal Points for Questions 1/1, 3/1, 4/1 and 6/1

⁷² [ITU-D SG1 Document 1/194](#) from Mexico

⁷³ ITU. Global Symposium for Regulators (GSR). GSR-19 Discussion Paper. [Building confidence in a data-driven economy by assuring consumer redress](#).

⁷⁴ United Nations. [The Age of Digital Interdependence](#). Report of the UN Secretary-General’s High-level Panel on Digital Cooperation. June 2019

⁷⁵ ITU-D SG1 Document [SG1RGQ/151](#) from India

Chapter 3 - Shaping a new framework for ICT consumer protection in the digital ecosystem

3.1 Protection vs innovation - How to protect consumers while still fostering innovation

Innovation is present in our daily routine when we watch video-on-demand on our mobile phones, use geolocation or interact with chatbots to search for information about a product or service. Sector dynamics change very fast and also affect consumer habits and needs. In this context, it is important to keep in mind that innovation is beneficial for end users in order to guarantee meaningful and secure use of ICTs, promote innovation for good, and foster healthy social interaction within a secure environment as well as a robust digital economy.

The creation of an environment for sustainable innovation bears a direct relation to the role of government regulation. Public choices regarding the need for government support or specific norms and guidelines directly impact on innovation. This is also the case for consumer-protection policy, where a miscalculated approach may favour or penalize a set of technologies or methods, affecting the final social result in terms of competition, welfare, creation of jobs, etc.

In this context, the debate must not simply touch upon the quantity of norms but also on quality and impact, while considering other relevant factors. At the end of the day, the benefits of regulation must be relevant to citizens. Also, it is important to consider that not only do governments and regulatory authorities have a role in tackling the big challenges of promoting innovation while protecting consumers, but also that no approach will succeed if it is carried out without permanent dialogue between governments and other national and international stakeholders, including private companies, civil society and international organizations.

Innovation, in this sense, must be present not only in relation to applications, services and technology, but also, very importantly, in relation to the way companies, governments and end users interact to benefit from technology and keep their rights protected.

OECD supports the implementation of impact assessments from the beginning of any regulatory procedure in order to identify information repositories, better assess the costs and benefits of possible interventions and consider alternative means for reaching the proposed objective. In this context, regulators around the globe have begun experimenting with techniques and methods involving careful observation of and insights into consumer behavioural patterns, allowing interventions to be tested in more or less controlled environments to reach faster and more cost-effective results.

The GSR-9 discussion paper on *Building confidence in a data-driven economy by assuring consumer redress* draws up international principles and recommendations.⁷⁶ One of them is related to consumer-protection themes in national strategies, which should consider:

- i. Building consumer trust
- ii. Ethical practices by providers of services and products with fair and equitable treatment, protection of privacy, disclosure and transparency
- iii. Development of fair, effective, transparent and impartial mechanisms to address consumer complaints through administrative, judicial and alternative dispute resolution, including for cross-border cases
- iv. Maintaining legal and/or administrative measures to enable consumers and organizations to obtain redress for the harm that they suffer as a consequence of goods or services which, for example, are defective, damage their devices, do not meet advertised quality criteria, or where there have been delivery problems and inappropriate circumstances involving non-monetary transactions
- v. Ensuring formal or informal redress procedures are expeditious, fair, transparent, inexpensive, accessible and do not impose a cost, delay or undue burden on the economic value at stake, and, at the same time, do not impose excessive or undue burdens on society and businesses; such procedures should take particular account of the needs of vulnerable and disadvantaged consumers
- vi. Co-regulation mechanisms among government bodies, market industries and consumer organizations to ensure that consumer protection enforcement authorities that handle consumer complaints have the ability to take action and obtain or facilitate redress for consumers, including monetary redress, while encouraging competition and removal of barriers to competition where they arise
- vii. Independent well-funded consumer advocacy forums to discuss overarching priorities for consumer protection
- viii. Consumers – in particular disadvantaged consumers – to benefit from new technology and new business models, with competition and regulation working together in the consumer interest
- ix. Education, awareness and digital skills programmes to be developed involving stakeholders from private, public and charity sectors, coordinating efforts to assist people to benefit safely from the digital economy
- x. Use of public buildings, such as libraries and local government buildings, to provide a trusted network of accessible locations with trained staff and volunteers, free Wi-Fi, computers, and other technology as well as assisted digital access
- xi. Performance scorecards for suppliers and digital comparison tools in regulated markets to hold them accountable for the outcomes they deliver
- xii. Providing the environment to ensure local priorities can be accommodated within a national framework.

Although these principles are particularly addressed to governments, some of them are also applicable to the private sector when building their mission, vision and commercial strategies.

It is necessary to recall that in a dynamic world of innovation it is impractical to establish a regulatory framework that covers all situations relating to consumer protection. Therefore, principles such as “consumer trust”, “ethical practices” and “development of transparency” are pivotal and must be followed by all stakeholders.

In this regard, an issue that emerges is how telecommunication operators are organizing their procedures and activities in order to ensure that the available technologies, tools and

⁷⁶ ITU SG1 Document [SG1RGQ/153+Annex from the BDT Focal Point for Question 6/1](#)

applications are being adequately used so that they can bring efficiency from the operator's perspective and, at the same time, guarantee trust and confidence from the end user's point of view. This seems to be the case when discussing automated calls, and the use of robot calls for commercial policies. It is not a reasonable option to forbid them. But, on the other hand, their abuse and uncontrolled use can be harmful for end users, be it in terms of annoyance or, more seriously, of their being used to perpetuate fraud. **Brazil** presented a contribution with a case study on that issue. After identifying unwanted calls as an increasing problem, an innovative approach based on enforced self-regulation was implemented. A code of conduct was established, including the implementation of a "do not call" list by which end users can block telemarketing calls.⁷⁷

3.2 Customer care (new technologies to facilitate customer experience)

Many countries have established in their legal framework that providers should give customer support by phone. In **Latin America**, Argentina, Brazil, Chile, Colombia and Mexico require fixed and mobile voice and data service providers to make helpdesk services available. Argentina, Brazil, Colombia and Mexico also regulate response time and ensure that helpdesk services are available free of charge. In **Europe**, Italy regulates both helpdesk availability and response time. The availability and access at any time for all customers does not mean that everyone will make use of customer care contact channels.⁷⁸

In fact, surveys in **Mexico**⁷⁹ show that most users do not contact their provider for any reason (complaints, doubts, failures, etc.). Only between 10 per cent and 30 per cent, depending on the service, admit they have contacted their provider. When it comes to complaints, 90 per cent say they have not filed any complaint.

Surveys in **Mexico** and **Brazil** show that those who contact their provider still prefer phone calls and face-to-face contact.

According to a Brazilian survey,⁸⁰ around 25 per cent of all complaints filed before the telecommunication regulator (Anatel) deal with failures of telecommunication operators to provide adequate and timely customer care. Consumers are not pleased with services provided by call centres, and this is a possible reason why low scores for call-centre services persist annually in Brazilian surveys. In Mexico, surveys have identified opportunity areas for improving customer services, which suffer from long waiting periods to contact phone operators and for technical visits, short or limited service hours, and unqualified personnel who offer incomplete information.

On the other hand, Brazilian surveys also point to shifting consumer behaviour and an increasing demand for self-care through the digital service channels.⁸¹ The digitalization trend in customer care opens up positive perspectives for user satisfaction and quality assessment along with the exercise of consumers' rights. The diffusion of mobile devices has provided the means for apps to become a major channel for consumers to voice their concerns.

⁷⁷ ITU-D SG1 Document [SG1RGQ/206 from Brazil](#)

⁷⁸ ITU-D SG1 Document [SG1RGQ/311\(Rev.1\)+Annexes](#) from Brazil

⁷⁹ ITU-D SG1 Document [1/186 from Mexico](#)

⁸⁰ ITU-D SG1 Document [1/219 from Brazil](#)

⁸¹ ITU-D SG1 Document [SG1RGQ/310 from Brazil](#)

In this context, technologies such as chatbots and virtual assistants, with the possible use of AI, play their part in tackling most of the ordinary and more voluminous demands. Developers seek to adapt these technologies to natural language, increasing the fluidity of conversation and seeking bonds with users. These interactions also generate large amounts of data on consumers themselves, providing operators with crucial intelligence for future interactions and paving the way for increased personalization of customer care.

Digitalization also points to the possibility of achieving positive results for regulators as they seek to embrace the use of technology for the dissemination of information and awareness campaigns. Examples include digital platforms for claim handling, which allow for filing and responding in a controlled digital environment, along with the subsequent publication of results regarding care provided. This increases transparency and contributes to lowering the incidence of disputes.

Nevertheless, all the highlighted benefits of the digitalization process that is being implemented in many countries have not so far been able to obviate the need for the regulator to act as a mediator between consumers and providers.

In general, regulators receive complaints and set deadlines for demands to be resolved. Some choose to mediate conflicts individually, others forward complaints to providers for them to respond directly to consumers within a given time-frame. The channels for receiving complaints range from phone calls, online forms, letters, e-mails and apps to personal contacts. For data consolidation, it is desirable that all complaints, irrespective of the input channel, be systematized in a single platform and the data publicized as a means for transparency as well as for comparison of service providers by end users. In addition to seeking to resolve individual consumer conflicts, regulators may also adopt forms of collective action, such as identifying the biggest causes of complaints to monitor, change/adapt frameworks and invoke punitive measures if irregularities are identified.

In **Benin**, ARCEP acts as a mediator between consumers and operators in a procedure that must not exceed 30 days. Complaints are received by phone or through the regulatory authority's website and recorded directly on a complaint-management platform. This enables the automated management of consumer complaints as well as the procedures and conditions for handling complaints by internal mediators, in a transparent, efficient and professional manner. The regulator's goal is to arrive at a solution to the disputes. As a result of the mediation, providers may be required to comply with applicable legal/regulatory obligations and to compensate for damages or take other remedial measures.⁸²

In **Brazil**, Anatel receives approximately 3 million complaints annually against telecommunication providers. Currently, the channels for receiving complaints free of charge are its website, app and call centre. If the problem is not solved after contacting the operator directly, the consumer can file a complaint with Anatel. As soon as it receives a complaint, Anatel forwards it to the impugned provider. The operator, not Anatel, is responsible for handling the request and for interacting directly with the consumer to solve the complaint within a 10-day period. Once the operator has responded conclusively, the consumer has 10 days to evaluate or re-open a complaint if it has not been resolved satisfactorily. If the consumer has neither evaluated nor re-opened the case within this time limit, the case will be considered finalized and the system will classify it as "resolved".

⁸² ITU-D SG1 Document [1/179](#) from Benin

Among other things, consumer complaints help Anatel to:

- i. Evaluate performance in attending to customer complaints and disseminate information
- ii. Identify the main problems of the operators and act in a preventive way, or even improve the existing rules
- iii. Carry out inspections and monitoring as well as control actions, when necessary.

In 2013, Anatel's call centre was the main channel, receiving 92.54 per cent of the demands registered. That same year, Anatel decided to invest in digitalization as a way of innovating technologically. After a migration strategy implemented in July 2020, digital channels already represent 61 per cent of total registrations.⁸³

Consumer behaviour has changed, and so the ways in which customer care services are rendered must adapt and innovate. Knowing more about the experiences of the consumer and the complaint journey is a fundamental condition for implementing the migration from helpdesk to digital services. Simplicity and availability of digital tools are key to effectively using these channels.

According to OECD, about 327 million fewer women than men have a smartphone with access to mobile Internet services and, on average, women are 26 per cent less likely to own a smartphone than men. According to UNCTAD, in two-thirds of all countries globally the proportion of women using the Internet is lower than that of men. Internet access is still limited by restrictions imposed by gender, age, disabilities and levels of education, among other factors, and the process of innovation and digitalization should take these aspects into account.

In other words, this confluence of interests requires challenges to be addressed, otherwise consumers will not be able to migrate to digital customer support tools. In fact, during the coming years, it seems that technology and human interaction must be employed together to solve customer-care demands. This combination will unite both the human capacity to create emotional bonds and the power of data processing and machine learning. The role of the regulator is expected both in the scope of regulation and in stimulating trust and ethical relations between all parties.

Although it is difficult to view recent history in the proper perspective, one cannot ignore the fact that the COVID-19 pandemic has impacted customer services in critical ways. The events have defined telecommunication infrastructure as a critical foundation for all sectors. The challenges are enormous and require varied solutions depending on the complexities faced by each country.

Among other challenges, it has become evident that consumer complaints and needs should be managed in a more proactive way and providers should work to ensure the accessibility and quality of subscription services. In this context, regulators, providers and consumers have been pushed to make use of ICTs to communicate and solve problems.

In the **State of Palestine**, which participates in ITU work under Resolution 99 (Rev. Dubai, 2018) of the Plenipotentiary Conference, the ministry has been interacting through WhatsApp and Facebook as channels for submitting complaints and remotely accessing queries from its officials. Subscribers have always had to visit a company showroom in order to obtain services and related information. But, with movement limited by restrictions and closures imposed as

⁸³ ITU-D SG1 Document [SG1RGQ/309](#) from Brazil

a result of the pandemic, contracts are inevitably being processed remotely with the help of technology. Although these are not viewed as a substitute for hard-copy contracts, it is as a solution that enables the provision of services without drawbacks for any of the parties.⁸⁴

In **Brazil**, with social isolation and the need for contactless options, the main telecommunication service providers reported a growth in digital channels, with emphasis on the use of their own apps, WhatsApp and virtual assistants.⁸⁵ Furthermore, Anatel created a crisis committee to oversee and monitor the impacts of COVID-19. In March 2020, the agency and telecommunication providers signed a public commitment to:

- i. Keep services running
- ii. Guarantee special support to health services and public security
- iii. Consider consumers' difficulties
- iv. Keep the population well-informed.

Considering the individual actions of the five main service providers, around 100 initiatives were implemented to facilitate access to payment methods, including: extra data allowances on mobile and fixed broadband, extra data allowances for prepaid services refill, access to a variety of contents without data usage caps (including the Health Ministry app about the coronavirus, in accordance with the public commitment signed with Anatel, and the government social benefits app).

Many countries, if not all, have general consumer laws in place. The laws cover a wide spectrum of consumer products. However, the law is generally slow in catching up with the ever-changing bouquet of technological changes, which has resulted in products that did not exist or were not envisaged when the laws were promulgated. The challenge for current legal frameworks is to protect consumers, promote innovation, enhance customer care, resolve cross-border problems, bridge the digital protection divide, cater for the advent of IoT and AI, and ensure that the framework facilitates online communication and transactions. While most of the general laws may not have been formulated with broadband services in mind, some of the problems the laws were drawn up to deal with and which already existed before the digital era are still current. Therefore, the laws remain very relevant and useful in the digital economy. This is evidenced by the laws in 12 countries that were examined in a contribution to the study group and discussed during the February 2020 Rapporteur Group meeting.⁸⁶

3.3 How to resolve problems arising from cross-border activities

The challenge to address cross-border activities has become even more strategic in the context of the global digital economy.

The digital economy is borderless, which implies a great deal of international transactions. For that reason, consumer protection and redress should be coordinated internationally. UN Member States, OECD and ITU have been working towards that goal. The *UN 2016 Guidelines for Consumer Protection* for online and offline commercial activities and dispute resolution and redress⁸⁷ is a fundamental tool to support consumer protection in that regard.⁸⁸ There appears

⁸⁴ ITU-D SG1 Document [SG1RGQ/307+Annex from the State of Palestine](#)

⁸⁵ ITU-D SG1 [Document SG1RGQ/360](#) from Brazil

⁸⁶ ITU SG1 Document [1/336 from Zimbabwe](#)

⁸⁷ UNCTAD. [United Nations Guidelines for Consumer Protection](#). New York and Geneva, 2016.

⁸⁸ ITU SG1 Document [SG1RGQ/153+Annex from the BDT Focal Point for Question 6/1](#)

to be international consensus that principles should be technologically neutral and that some specific areas require more attention, such as the ordering of online goods and services, data protection, spam and fraud.

Considering its size and scope, the European Union can be seen as a useful paradigm for resolving some problems relating to cross-border activities. As of June 2017, the EU has put an end to roaming charges and this measure has served as an example to other jurisdictions. A constant issue relating to roaming is the phenomenon known as “bill shock” and the European policy seeks to prevent its occurrence by focusing on temporary travel (“roam like at home”).

The General Data Protection Regulation (GDPR) is another initiative where the EU has demonstrated the benefits of a common approach to cross-border activities. The regulation provides for the need to inform users of possible international flows of data, creating a personal right to information regarding the use of personal information.

Another cross-border emerging issue is unsolicited commercial communications, or nuisance calls. In a global digital economy, digital tools and telephones are expected to be a way of facilitating economic exchanges between those offering a product or a service and their potential buyers. However, while some economic agents operate within ethical and fair boundaries in this environment, others do not, flooding users with unwanted calls. In addition to commercial calls, some callers aim at harming the receiver through misleading and fraudulent practices. Many countries around the world have been facing this problem and different approaches have been adopted, which include network call traffic, call authentication systems, definition of telemarketing prefix numbering, legal changes and do-not-disturb lists. These are outlined in a contribution from **Brazil** giving an overview of challenges and strategies in relation to unwanted calls.⁸⁹

In **India**, the Telecom Regulatory Authority of India (TRAI) announced the directive under TCCCP (Telecom Commercial Communications Customer Preference) regulations to put in place a blockchain technology-enabled platform.⁹⁰

In **Brazil**, the NRA (Anatel) and telecommunication operators addressed the problem of nuisance calls through a self-regulatory (including self-enforcement mechanisms) and responsive approach. The operators presented to Anatel a code of conduct for offering telecommunication services through telemarketing, and also implemented a single national do-not-disturb list.⁹¹

The ITU-D study groups held a webinar on “Unsolicited commercial communications/nuisance calls: Are consumers more vulnerable in the era of COVID-19?”⁹²

During the webinar, the United States Federal Communications Commission (FCC), the Brazilian National Telecommunications Agency (Anatel) and Idea-Vodafone (India) shared their national approaches on dealing with the issue. The importance of consumer education was emphasized. Beltug (Belgium/Europe) drew attention to the fact that users are more vulnerable in times of crisis, such as the COVID-19 pandemic, with an increase in electronic fraud by phone as well as by e-mail. In this context, the demand for security is increasing. The African Telecommunications

⁸⁹ Document [SG1RGQ/308 from Brazil](#)

⁹⁰ Document [1/334 from India](#)

⁹¹ ITU-D SG1 Document [SG1RGQ/206 from Brazil](#)

⁹² ITU-D. ITU Webinar on [Unsolicited Commercial Communications / Nuisance calls: Are consumers more vulnerable in the era of COVID-19? 2 July 2020.](#)

Union (ATU) highlighted the importance of a cross-border vision, including an international plan to establish standards to deal with the issue.

ITU-D Study Group 1 Question 6/1 proceeded to use the contents of the workshop to enrich its annual deliverable entitled “*Unsolicited Commercial Calls – An overview of Challenges and Strategies*”,⁹³ which was approved in September 2020 and released thereafter.

3.4 How to meet the needs of persons with disabilities and of women and children in a new digital ecosystem (technologies, services and products focusing on consumer protection and digital literacy relating to consumer protection)

The ICT consumer public includes several vulnerable groups who have specific needs regarding equality and access.

The GSR-19 Discussion Paper *Building confidence in a data-driven economy by assuring consumer redress* relating to consumer protection in a digital age, proposes the following recommendation:⁹⁴

Recommendation 4: National principle-based digital policy – Government should, after public consultation, develop a strong consumer-centric, principle-based, national digital strategy and implementation plan. The objective of the digital plan is to enable all consumers, including people with disabilities, businesses and government to safely take part in the digital economy. The implementation plan should contain incentives to ensure every person has available skills to use high-speed Internet connectivity and take advantage of the digital economy whilst minimizing risk of harm.

Reducing barriers is a central question when it relates to persons with disabilities, a group which comprises around 10 per cent of the world population according to the World Health Organization (WHO). A user-centric approach is crucial to the development of products and services for those with physical, visual, hearing, mental or intellectual disabilities. User-centric design allows for not only seeing accessibility in physical terms, but also recognizing its cultural peculiarities.

The evidence collected through surveys in **Mexico** shows that about 70 per cent of persons with disabilities do not know about their rights when hiring services. In addition, surveys have enabled IFT (Mexico) to recognize and publish the main areas of opportunity that users with disabilities identify, such as providing treatment according to their needs, providing specific information about equipment, software or packages to facilitate their use, and providing communication (brochures, advertising and promotions) in accessible formats.⁹⁵

In **Brazil**, there are around 45 million people with some disability, representing more than 23 per cent of the population. This fact is a great driver for improving accessibility in telecommunications by using new technologies. In this context, Anatel published the *General Regulation on Accessibility – RGA (Resolution 667/2016)*, based on the Rights of Persons with

⁹³ ITU-D Study Group 1. Question 6/1. Annual Deliverable 2019-2020. [Unsolicited Commercial Communications – an overview of challenges and strategies](#).

⁹⁴ ITU SG1 Document [SG1RGQ/153+Annex from the BDT Focal Point for Question 6/1 and ITU. GSR-19 \(op. cit.\)](#)

⁹⁵ ITU-D SG1 Document [1/186 from Mexico](#)

Disabilities – Law N° 13.146/2015. In regard to the rights of disabled persons and obligations of telecommunication companies, RGA obligated companies to prioritize and individualize accessible service for disabled persons and their personal companions; offer physical documents (contracts, service plans, among others) in an accessible format for visually disabled persons; maintain websites under an accessible format; and maintain webchats and video calls through the Internet.

Moreover, this framework also created an accessibility ranking index. The idea is to reward companies annually which, in addition to complying with the rules established in the RGA, maintain best practices to promote the inclusion of people with disabilities. Anatel gave the award to an operator for the first time in 2019. The five major companies were evaluated according to the following criteria: accessibility on websites; specialized service in stores; efficiency of the mechanism of interaction through electronic messages, webchats and video calls; and volunteer actions that encourage/promote/guarantee the rights of persons with disabilities.⁹⁶

When one considers the accessibility gap from the point of view of gender, challenges are slightly different. The proportion of women who use the Internet is 12 per cent lower than that of men, and in the mobile segment women have in general 26 per cent less probability of using the Internet than men. Some aspects of technological change pressure women the most: local context, digital illiteracy, physical security and the cultural perception that the Internet might not be relevant to one's life.

The young (less than 18 years old) constitute one-third of Internet users today, and persons between 15 and 24 years old are the most connected demographic group. Nowadays, even children much younger are connected.

In **Japan**, KDDI Corporation is promoting the *Smartphone Safety Classes* initiative. According to the National Police Agency, the number of students victimized by the social networking service (SNS) is increasing almost at the same rate as smartphone penetration for school students. KDDI Corporation conducts classes as an initiative to ensure that students (primary, secondary and high school) can safely and securely use communication devices, such as smartphones, without getting into trouble. The classes cover consumer protection topics, such as "spreading misinformation", "writing hurtful comments on social media", "trusting people too easily online", "bullying through SNS", and "game and SNS dependence on smartphones". Between 2005 and 2019, a total of 29 000 classes have been held with over 5 310 000 attendees.⁹⁷

Around 346 million young people are still not connected to the Internet. This is a major policy concern as this gap generally prevents this generation from pursuing educational and professional qualifications. Moreover, the importance of having proper policies and actions to protect children in the online environment should be highlighted.

ITU's Child online Protection (COP) initiative is aimed at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere. Likewise, the Global Kids Online (GKO) initiative launched by UNICEF deals with the issue of protecting children online.

⁹⁶ ITU-D SG1 Document [SG1RGQ/196 from Brazil](#)

⁹⁷ ITU-D SG1 Document [1/397 from KDDI \(Japan\)](#)

The **Islamic Republic of Iran**⁹⁸ points to risks related to the use of ICT services by children and presents some approaches related to COP, among them the integration of children's rights in all policies related to ICTs, including training children, parents and teachers in the safety of children and their responsibilities in using ICTs. Also, it mentions the need for parental controls and cyberspace management tools to protect children in cyberspace.⁹⁹

In this sense, the Iranian ICT Ministry has developed and published a policy called Supportive document and action plan for the development of children's Internet services.¹⁰⁰

The plan outlines four goals:

- i. Providing communication, content and trust infrastructure
- ii. Developing the market and growing businesses
- iii. Cultivating education and promoting cyberspace
- iv. Management action plan.

In order to promote access to all these groups, filling in the gaps is crucial. In 2019, the Federal Telecommunications Institute (IFT) of **Mexico** started a digital literacy programme called *Conoce tus derechos* ("Know your rights"). The programme employs learning courses, talks and information desks to empower consumers to know and identify their rights as users of telecommunication services and ways to make them enforceable. It fosters the importance of making informed decisions and proper use of telecommunication services and equipment.¹⁰¹

Digital plans aim to reduce barriers to communication.

In this context, the **Russian Federation** extended the principle of "roam like at home" by decree to all mobile telecommunication operators and introduced the requirement of free incoming calls.¹⁰²

The National ICT Authority (NICTA) of **Papua New Guinea** is in the process of establishing a regulatory framework for QoS. One of the aims is to help consumers understand any QoS differences that may exist between different service providers, empowering them to take such information into account when choosing a service provider.¹⁰³

3.5 AI, IoT and other emerging technology users: A new category of activities and players needing new tools

New digital technologies, such as artificial intelligence, hold the potential to greatly improve lives. Apart from a host of applications in health, education, mobility, agriculture and manufacturing, AI can also improve digital communication services and enhance consumer experience.

According to different sources, the current state of adoption of AI and IoT as it impacts the end user today represents only a small fraction of the full potential of the technologies. Nevertheless, although the potential use of the technologies may be beyond the grasp of the ordinary

⁹⁸ ITU-D SG1 Document [SG1RGQ/196 from Brazil](#)

⁹⁹ ITU-D SG1 Document [1/76](#) from Iran University of Science & Technology (Islamic Republic of Iran)

¹⁰⁰ ITU-D SG1 Document [1/74 from Iran University of Science & Technology \(Islamic Republic of Iran\)](#)

¹⁰¹ ITU-D SG1 Document [1/349](#) from Mexico

¹⁰² ITU-D SG1 Document [1/317 from the Russian Federation](#)

¹⁰³ ITU-D SG1 Document 1/329 from Papua New Guinea

consumer, some issues are being discussed in depth by consumer associations, individuals and regulators.

Commercial applications of AI and IoT presented so far are based on data generated by machine-to-machine (M2M) and human-to-machine (H2M) interactions. This raises questions regarding the protection of user data, across border jurisdictions – the international flow of data – but also the legal boundaries between regulated and non-regulated sectors of the economy. Even the usual distinction between trade in goods or services may not be applicable in this context.

As of today, irrespective of the economic sector in which AI and IoT are operating, transparency for the consumer arises as a central question, given the information asymmetry between the users and providers of goods and services. This point revolves around knowing which data are being collected, when, and how they will be used in the future. Other data-related concerns about AI and IoT deal with algorithm transparency – the risk of identification of individuals through data, asymmetry in data aggregation, possible racial and social bias, security-by-design, cyberthreats concerning interconnected devices, protection of children and product warranty, among others.

These challenges were pointed out by **India**¹⁰⁴ and **Zimbabwe**¹⁰⁵. Both countries highlighted the importance of well-established national privacy and security policies as well as rules regarding AI and IoT so that consumers remain protected. Moreover, as with other consumer-protection issues in the digital age, issues emanating from the use of AI and IoT also require regulatory collaboration and capacity building both at the national and international levels. The ultimate aim is to harness the benefits of technology, while safeguarding against potential harm.

¹⁰⁴ ITU-D SG1 Document [1/307 from India](#)

¹⁰⁵ ITU-D SG1 Document [1/336 from Zimbabwe](#)

Chapter 4 – Fostering consumer empowerment and awareness (competition, business models and prices, and transparency)

4.1 How can consumers be empowered to participate in the digital economy?

How can regulators help to raise awareness and empower consumers in the new digital ecosystem?

Helping consumers to acquire the skills necessary to use digital services is a prerequisite for the development of the digital economy. Indeed, while digital innovation and competition within telecommunication markets have improved consumer empowerment, regulators still have an important role to play in helping to raise awareness and empower consumers in the new digital ecosystem.

Promoting full connectivity will enable demand for high-quality services on the part of consumers, supported by the very high-capacity networks whose development is a key priority in creating positive interactions. Also, national regulatory agencies should continue to work in promoting choice and empowerment for end users, by prioritizing work to build trust in ICTs and digital services and to enable and result in better informed choices by consumers.¹⁰⁶ To that end, they could, for example, compel digital service suppliers to publish relevant information on their services and to design tools that raise awareness among end users, helping them to make a choice.

Regulators' approach to empowering end users could be constructed around two pillars:¹⁰⁷ monitoring of the sector and the appropriate level of transparency. As part of monitoring the functioning of the electronic market, regulatory authorities could also monitor new end-user provisions, such as information provision requirements, including the contract summary template. In terms of transparency, regulators could also continue to work towards greater involvement of stakeholders, including consumer representatives.¹⁰⁸

Moreover, institutional and international cooperation between national regulatory agencies around the world can be an important means to strengthen the capacities of digital consumers by sharing experiences and good practices.

Regulators can help raise awareness and empower consumers through a combination of actions. These include collaboration among the many stakeholders to produce relevant policies, strategies, laws, regulations, guidelines, redress processes and enforcement. Service providers

¹⁰⁶ BEREC. [Report on transparency of tariff information](#). Document ERG (08) 59rev2. March 2009.

¹⁰⁷ Ibid.

¹⁰⁸ Ibid.

need to comply with laws and be socially responsible. Consumers must be digitally educated and made aware.

Finally, among the regulatory interventions available in the scope and competence of NRAs is the possibility to compel suppliers to publish information for the benefit of consumers.

Corporate best practices in favour of consumers of telecommunication services

Some service providers in the communication sector have developed self-regulation practices that include the development of a consumer bill of rights, provide adequate and accurate information to consumers that enable them to exercise effective choices and assert their rights, and put in place transparent and low-cost procedures to make it easier for consumers to change service providers.

Others, in conjunction with policy-makers and regulators, assist consumer participation in telecommunication markets by educating consumers about their rights, by raising awareness about new services and options offered by the market, and by making the process of switching in the fixed line, mobile and Internet markets easier, cheaper and faster.

4.2 Transparency as a mechanism to promote competition on tariffs and quality of service

4.2.1 Comparison tools for transparency and consumer empowerment

According to BEREC, some negative consequences in using telecommunication services can be prevented by giving consumers access to information that is relevant to their needs.

In the *Report on transparency of tariff information*, BEREC states that information practices can be divided into three categories, according to the party which provides information to end users:

1. Information methods/tools employed by service providers
2. Information methods/tools implemented by NRAs
3. Information methods/tools made available by third parties.

As for the first category, BEREC affirms that a wide range of methods and tools are used by providers of electronic communications services to inform end users on either a mandatory or voluntary basis. There is also a mix of static and interactive instruments. Measures considered by some NRAs to be particularly effective in the first category include publication on providers' websites, bills (in particular, itemized bills with a regulated minimum content), or leaflets sent along with them.¹⁰⁹

The instruments in the second category generally target individual consumers, offering online and/or personalized assistance. Some NRAs have rated as being particularly effective customer care service, instant billing control applications, voice announcements/acoustic signals when calling a ported/off-net/special tariff number, and information sent via SMS or e-mail directly to the user.

The BEREC report shows that tools providing direct information to consumers in a targeted and personalized way (via phone, letters, e-mails, SMS, interactive web applications, etc.) can

¹⁰⁹ Ibid.

complement the general information requirements to be met by providers, in particular in relation to changes occurring after the entry into a contract and controlling expenditure on electronic communication services. Web-based methods can be complemented by “offline” methods able to reach a wide audience, especially where many in this audience may not have access to the Internet. Implementation of such methods – either compulsory (by law or regulation) or voluntary (via encouraging and guiding industry self-regulation) – can empower end users, helping them make informed choices which best serve their needs.¹¹⁰

Some NRAs have put in place a variety of methods, approaches and tools to inform digital consumers. These include static and unidirectional (such as publication of general information on websites maintained by NRAs), dynamic and unidirectional (through media campaigns) and dynamic and bi-directional or interactive (offer comparison websites, consumer assistance via telephone, mail or e-mail, etc.) approaches.¹¹¹

NRA websites can be regarded by many regulators as effective information tools. Most NRAs publish general end-user information on their websites, including the possibility of switching between providers, the rights of end users in dealing with service providers, complaint and dispute settlement procedures, advice on choosing an offer, generalities on tariffs and billing, and special charging rules. Other tools considered to be effective information tools by responding NRAs are interactive web-based price guides (“price calculators”), which can perform calculations based on preferred consumption volumes and rank subscription packages from different providers according to their price. Overall, half of the NRAs have introduced or consider it appropriate to introduce such tools, directly or through the accreditation of third-party initiatives.¹¹²

Successful price calculators that cover the full range of electronic communication services are rich in features but, at the same time, display a particularly user-friendly interface and attach significant value to the simplicity and ease of the user experience. An alternative to an NRA running an interactive price calculator or website is where the NRA establishes a system for the accreditation of such websites maintained by third parties.

Moreover, an accreditation scheme can provide quality assurance, for example by certifying that the price calculations offered by accredited websites are accessible, accurate, transparent and comprehensive. Other information methods rated as effective by NRAs include the use of media channels (radio, TV, newspapers), the distribution of leaflets, and the use of individual communication channels where end users can seek assistance.¹¹³

These tools may have particular relevance for those who do not have access to the Internet and can complement the use of web-based information instruments.

National and international third parties may also be useful in developing complementary initiatives to those deployed by service providers and NRAs in their effort to inform end users.

¹¹⁰ Ibid.

¹¹¹ Ibid.

¹¹² OECD. [Toolkit for protecting digital consumers: A resource for G20 policy-makers](#). OECD, 2018. (op. cit.)

¹¹³ Ibid.

4.2.2 Concrete examples of how regulators can raise awareness and communicate results of performance-monitoring exercises and consumer assessments to consumers (to keep consumers and users informed about the basic features, quality, security and rates of various services being offered by operators)

Concrete examples of how regulators can help raise awareness are given below.

In **India**, the Telecom Regulatory Authority of India (TRAI) aims to empower consumers of telecommunication and broadcasting services by way of transparency in the systems being run by telecommunication service providers (TSPs). TRAI has taken a number of initiatives in this regard, including setting a benchmark for wireless data networks as well as assessing network performance on a periodic basis. TRAI introduced a mobile app 'TRAI my speed' to enable users to measure broadband speed and report it to TRAI on near real-time basis. While measuring broadband experience is important for enabling consumers to make an informed choice, it also helps regulators and policy-makers assess the accessibility of services dependent on a broadband connection.¹¹⁴ The broadband experience across geographic locations and various networks also provides insights into the extent and level of achievement of the goals set by the government.

In accordance with Resolution 196 (Rev. Dubai, 2018) of the ITU Plenipotentiary Conference¹¹⁵ and Resolution 64 (Rev. Buenos Aires, 2017) of WTDC,¹¹⁶ the **Russian Federation** is taking a series of measures to establish a QoS system for telecommunications/ICTs and is engaged in activities to protect the key interests of communication service consumers, thereby helping providers and consumers of telecommunication/ICT services interact on an equal footing.¹¹⁷

These efforts include the development of a government policy to protect the rights of telecommunication/ICT users and consumers, particularly in relation to obtaining free and up-to-date information on telecommunication service rates and conditions and international roaming charges, and to ensure high-quality telecommunication/ICT services for all by introducing a system of government standards defining quality-of-service indicators.

In **Ghana**, all operators are obligated to publish information on how the mobile services on tariff plans are rated in any two nationally circulated newspapers and also on the service provider's website. The details of these tariff plans, taking into account the terms and conditions, are collected and the business rules are fed into a SIGOS SITE-rating engine, which is equipped with subscriber identification modules (SIM) subscribed on various promotions and offers.¹¹⁸

It is also important for regulators and policy-makers, particularly in times of emergencies such as COVID-19, to provide guidance and input to stakeholders on possible updates in subscription contracts so as to reflect the evolution in services prompted by the global pandemic, the impact of which has been immense on the sector. In the **State of Palestine***, for example, the Complaints and Consumer Protection Unit conducted a thorough review of subscription services with the

¹¹⁴ ITU-D SG1 Document [SG1RGQ/182](#) from the Telecom Regulatory Authority of India (TRAI) (India)

¹¹⁵ ITU. Plenipotentiary Conference. Resolution 196 (Rev. Dubai, 2018), on protecting telecommunication service users/consumers. [Final Acts of the Plenipotentiary Conference \(Dubai, 2018\)](#), p.399.

¹¹⁶ ITU. WTDC Resolution 64 (Rev. Buenos Aires, 2017), on protecting and supporting users/consumers of telecommunication/ICT services. [Final Report of the World Telecommunication Development Conference \(Buenos Aires, 2017\) \(WTDC-17\)](#). Buenos Aires, Argentina, 9-20 October 2017. p. 507.

¹¹⁷ ITU-D SG1 Document [SG1RGQ/201](#) from the Russian Federation

¹¹⁸ ITU-D SG1 Document [SG1RGQ/244](#) from Ghana

aim of guaranteeing access for subscribers to their full rights and the services they request. The Ministry also provided WhatsApp numbers for subscribers to submit complaints and queries to officials.¹¹⁹

4.3 How can consumers defend their rights more effectively (concrete examples of mechanisms to protect consumers on selected issues enabling them to know and exercise their rights, to use the services properly, and to make informed decisions when contracting services)

4.3.1 Means to prevent fraudulent, deceptive and unfair commercial practices, transparency and subscription agreements

Studies have shown that many of the service providers' promotional campaigns fail to provide consumers with the basic information required to make an informed choice as to which service they should subscribe to, including the key element of any such promotion – the price.

In recent years, the number of promotional campaigns run by mobile telephone companies and the fixed service company in the **State of Palestine** along with the level of competition among providers of Internet services on the access line have increased to such an extent that companies have begun using incentives to drive their promotional campaigns.

These types of campaigns, including daily, weekly and monthly offers, are new to the country, presenting consumers with a wide range of options to meet their needs. This has prompted the Ministry to organize a number of intensive oversight campaigns for the telecommunication and ICT market.¹²⁰

Unsolicited calls are both a national and cross-border affair, reaching many sectors of the economy worldwide.

Considering the absence of federal regulation on the subject of unsolicited calls, Anatel in **Brazil** chose to address the issue of unwanted connections from the telecommunication sector, assuming the possibility of enforced self-regulation.¹²¹

The approach to curb the issue of unsolicited commercial communications (UCC) adopted in **India** is a noteworthy balanced approach. On one hand, it respects the privacy and wishes of subscribers, giving them control of the content, timing and mode of telemarketing communications and, on the other, it is telemarketing-friendly to the extent that it allows all stakeholders, such as access providers, registered telemarketers and business entities, to carry out their operations with transparency and within the framework of regulations.¹²²

¹¹⁹ ITU-D SG1 Document [SG1RGQ /155](#) from the State of Palestine*, which participates in ITU work under Resolution 99 (Rev. Dubai, 2018) of the Plenipotentiary Conference.

¹²⁰ Ibid.

¹²¹ ITU-D SG1 Document [SG1RGQ/206](#) from Brazil

¹²² ITU-D SG1 Document [SG1RGQ/182](#) from TRAI (India)

4.3.2 Best practices and tools to empower users/consumers and raise awareness on how they can manage their personal data

The widespread use of electronic services can make consumers more vulnerable, and increases the risk of identity fraud or damage to property. Moreover, free access to personal data on the Internet, lack of trained human resources to implement legislation effectively, and ineffective consumer associations are added challenges.

Online reputation defamation via social media, fraud (financial fraud, identity fraud, network fraud, etc.), misinformation and fake news have become frequent and increasingly more dangerous for consumers who are often poorly educated and have little comeback. They take advantage of the low costs touted by social media and OTTs in exchange for making personal data available.

In order to address this issue, **Guinea** passed legislation in 2016, which includes an act on cybersecurity and personal data protection and an act on electronic transactions. A personal data protection commission is being set up.¹²³

However, it must be noted that the rapid and significant development of information technologies requires - in addition to a legal framework - management, information and education in using information technologies.

Setting up commissions, developing skills and building capacity in data protection and management, and following up on problems and consumer complaints, should also be made a priority so as to ensure better protection for consumers and the exchange of best practices among various players in the sector.

On 31 December 2018, the Government of **Burkina Faso** adopted new regulations on ways of identifying electronic communication service subscribers and cybercafé customers.¹²⁴ The new regulatory framework is intended to help prevent ICT services from being misused for criminal purposes and to protect ICT consumers. The adoption of this decree will help fight insecurity by allowing the competent bodies and authorities to access a reliable database of electronic communication users. It will also help build confidence among ICT service consumers. The aim of this regulatory framework is to prevent providers from engaging in deceptive practices related to the collection and use of consumers' personal data.

As mentioned in section 2.4.1 above, **Brazil** has adopted legislation on personal data protection: Law N° 13.709, approved on 14 August 2018.

¹²³ ITU-D SG1 Document [SG1RGO/191](#) from Guinea

¹²⁴ ITU-D SG1 Document [SG1RGO/172](#) from Burkina Faso

4.3.3 Mechanisms/means put in place by regulators so that operators/service providers publish transparent, comparable, adequate, up-to-date information on, inter alia, prices, tariffs, and expenses related to contract termination, and accessing and updating telecommunication services in order to keep consumers informed and to develop clear and simple offers as well as best practices for consumer education

The drastic changes in the telecommunication/ICT sector have led national regulatory authorities and policy-makers to review their current regulations and policies regularly in order to enhance transparency in the new digital environment.

In **Ghana**, billing issues, including unjustified credit deductions, overcharging and wrong billing topped the list of complaints to the regulator, with consumers often feeling exploited as they were not getting value for their money spent on loading airtime on their mobile accounts. In this regard, Ghana introduced the Billing Feedback Message (BFM), an end-of-call notification via unstructured supplementary service data (USSD), or flash message, that informs the mobile-service user about how much airtime, SMS or bandwidth is consumed at the end of a billable activity. The purpose of the BFM was to address consumer complaints and the perceived inaccurate billing of telecommunication services.¹²⁵

4.3.4 Identification of best practices for national regulators and operators in the use and management of national telephone numbering resources

Faced with the rapid evolution of technologies and the appearance on the market of ever more sophisticated equipment, consumers who are not telecommunication/ICT experts can find themselves at a loss. Consequently, consumer information and consumer rights have become a priority, and the World Telecommunication Development Conference (Dubai, 2014) took account of the wish of Member States and Sector Members to study the protection of telecommunication/ICT consumers.

The issue of consumer protection has become a constant concern. Yet neither regulators, operators and service providers nor equipment manufacturers have defined or provided a specific legal basis for consumer-protection instruments that need to be implemented to guarantee universal access to quality telecommunication/ICT services at low cost.

The deployment of new technologies and the introduction of new services have increased the demand for numbering resources. This has raised the need for an adequate National Numbering Plan for effective competition and to meet future demands.

The regulatory approach with respect to the assignment, allocation, withdrawal and use of numbers, creating the possibility for number portability and carrier selection, should enhance competition in telecommunication markets.

¹²⁵ ITU-D SG1 Document [SG1RGQ/244](#) from Ghana

Chapter 5 – Conclusions and guidelines

After analysis of contributions presented, the following conclusions were reached and the following guidelines formulated:

5.1 Conclusions

- There is a growing risk of online fraud and misuse of personal data and ever-increasing complexity of online transactions and related terms and conditions.
- The regulation of online content has attracted regulatory measures, ranging from the adoption of self-regulation by intermediaries/platforms and the regulatory enforcement of a code of ethics, to imposing liability to screen out harmful content.
- Many elements and stakeholders make up the digital economy and digital ecosystem. Consumer protection principles and policies as well as recommendations and standards adopted at the international and regional levels can guide policy-makers and regulators at the national level, especially in an increasingly interconnected world.
- The COVID-19 response has shown an increased need for inter-agency, regional and international cooperation.
- Many, if not all, countries across the world have general consumer laws in place covering basic consumer issues related to the provision of most telecommunication services.
- Laws and regulations are generally slow in catching up with the ever-changing bouquet of technological changes. This has resulted in a lack of regulations governing products which did not exist or were not envisaged when the laws were promulgated.
- Very little has been done in many countries to come up with legislation to protect consumers in the development of AI and IoT.
- Personal data protection, privacy, the right to information, ethical billing, fair contract clauses, number portability, universal access, confidentiality, speedy complaint resolution, quality of service, radiation protection, child online protection, fair advertisements and the safe use of the Internet are key elements of any laws that seek to protect consumers.
- The challenge for current legal frameworks is to protect consumers, promote innovation, enhance customer care, resolve cross-border problems, bridge the digital protection divide, cater for the advent of IoT and AI, and ensure that the framework facilitates online communication and transactions.
- The nature of consumer protection in the area of converged services has consequently changed and will continue to do so because of rapid technological changes, the emergence of new services and their widespread uptake.
- Regulatory response can no longer be symmetric, given the vast variety of services and applications. There can be no one-size-fits-all solution. Regulators need to exercise caution so as to avoid hindering innovation and the growth of digital services. Yet, consumer safety and trust are equally important issues that need to be addressed if the pace of growth is to be sustained.
- Institutional and international cooperation between national regulatory agencies around the world can be an important means to strengthen the capacities of digital consumers by sharing experiences and good practices.
- The widespread use of electronic services can make consumers more vulnerable and increase the risk of identity fraud or damage to property. Moreover, free access to personal

data on the Internet, lack of trained human resources to implement legislation effectively and ineffective consumer associations are added challenges.

5.2 Guidelines

The following guidelines emanate from the study:

- Policy-makers should create a conducive environment through regulation and necessary legislation that will discourage service providers from short-changing consumers.
- Protection of consumers from online fraud and the misuse of personal data should be an integral part of regulatory policy.
- Consumers themselves should also be cautious and take necessary precautions, including installing and updating antivirus software, changing passwords, backing up information regularly, and connecting only to secure public networks.
- Since the digital economy is borderless, there is a need for cross-border cooperation among regulators.
- Consumer education on rights and obligations should be at the centre of policy-making.
- Legal frameworks need to be developed to protect consumers, promote innovation, enhance customer care, resolve cross-border problems, bridge the digital protection divide, cater for the advent of IoT and AI, and ensure that the framework facilitates online communication and transactions.
- Regulators need to exercise caution so as to avoid hindering innovation and growth of digital services.
- Investment in connectivity in rural and remote areas is now critical to enable individual and household connectivity, as pandemics and natural disasters can prevent people from getting access to broadband services through communal access points.
- Robust data protection frameworks should be put in place if unwanted calls and unsolicited communication are to be minimized.
- To achieve digital transformation, policy and regulation should be more holistic. Cross-sectoral collaboration should be encouraged along with revisiting regulatory approaches, such as co-regulation and self-regulation. This could lead to new forms of collaborative regulation based on common goals, such as social and economic good and innovation.
- Policy and regulation should be based on consultation and collaboration. In the same way that digital cuts across economic sectors, markets and geographies, regulatory decision-making should include the expectations, ideas and expertise of all market stakeholders and players, including academia, civil society, consumer associations, data scientists, end users, and relevant government agencies from different sectors.
- Policy and regulation should be evidence-based. Evidence is critical for creating a sound understanding of the issues at stake and identifying the options going forward as well as assessing their impact. Appropriate authoritative benchmarks and metrics can guide regulators in rule-making and enforcement, enhancing the quality of regulatory decisions.
- Policy and regulation should be outcome-based in order to address the most pressing issues, such as market barriers and enabling synergies. The rationale for any regulatory response to new technologies should be grounded in the impact on consumers, societies, market players and investment flows as well as on national development as a whole.
- Policy and regulation should be incentive-based, rewarding players who uphold consumer protection.
- Finally, setting up institutions such as consumer education centres, dedicated consumer complaint-handling centres or commissions and setting up dedicated consumer courts is recommended in order to protect consumers effectively.

Annex 1: Summary of contributions submitted to Question 6/1

Document [1/43 \(Brazil\)](#) presents the Brazilian consumer satisfaction and perceived quality regulatory framework, and defines lessons learnt which can be beneficial to Question 6/1. Under this framework, Anatel coordinates the annual survey of consumers and is mandated to enforce such obligation on operators. The aim of the survey is to provide greater transparency to consumers to inform their decision-making process in choosing an operator.

Participants requested clarification and further information on the practical tools Anatel uses to measure and evaluate consumer satisfaction, examining whether consumer associations are included in the survey and evaluation, how the cost of the survey is covered, and how this consumer satisfaction survey interlinks with other surveys and audits, such as those related to QoS. They suggested that such experiences could be shared in future contributions, including through case studies and other contributions. The contribution was noted.

[Document 1/45 \(Mexico\)](#) presents the *Users' Information and Empowerment System*, designed and implemented by the *Instituto Federal de Telecomunicaciones* (IFT) through its dedicated consumer affairs department (CGPU). The *Users' Information and Empowerment System* includes a set of online applications and is intended to provide telecommunication service users with the tools and elements needed for better decision-making when accessing, signing up for and using services by helping to eliminate asymmetries in information and train empowered users. The contribution was noted.

Document [1/74 \(Islamic Republic of Iran\)](#) from **Iran University of Science and Technology** (IUST) describes the general framework and action plan for Child Online Protection that has been developed in the country to support and harmonize activities related to Child Online Protection that have been conducted by the private sector and governmental organizations. The contribution was noted.

Document [1/76 \(Islamic Republic of Iran\)](#) suggests a number of categories of tools that could be considered in relation to Child Online Protection and proposes that the definition of such categories of tools (e.g. content refinement, applicable controls, monitoring) as well as best practices and case studies could be the subject of a survey (questionnaire), the results of which could be included in the final report of Question 6/1. The contribution was noted.

Document [1/48 \(BDT\)](#) contains a series of resources and materials that have been developed and that could be useful for the activities of the ITU-D study groups, in particular for Study Group 1 Question 6/1. The contribution was noted.

[Document 1/84 \(BDT\)](#) shares information on the lessons learned as indicated by members in their contributions to the first meeting of ITU-D Study Group 1 for the 2018-2021 study period. The contribution was noted.

Document [SG1RGQ/20 \(Brazil\)](#) presents the Brazilian experience on an alternate and experimental approach to enforce consumer protection and rights. It particularly highlights Anatel's experience in addressing the billing of unwanted value-added services (VAS) from mobile-phone consumers. Participants requested further clarification on the tools required and shared relevant experience in their countries.

Document [SG1RGQ/31 \(Madagascar\)](#) highlights the importance of adopting a digital identification policy which includes the registration of SIM cards in order to enhance access

to mobile services. The contribution further shares experience from Madagascar on the identification of SIM card users, which has become essential for interconnection of services. Madagascar also introduced the obligation for operators to introduce awareness-raising activities.

Document [SG1RGQ/34 \(India\)](#) stresses the importance of addressing the culture of security that promotes trust in telecommunication/ICT applications and services, and the effective enforcement of privacy and consumer protection. The contribution calls for Question 6/1 to include “Best practices and tools to empower users/consumers in managing their data provided to telecommunication service providers” in this cycle, as provided in the Buenos Aires Action Plan.

Document [SG1RGQ/52 \(India\)](#) emphasizes the importance for industry, regulators and academia to address data protection, privacy, competition and security, and develop an appropriate regulatory framework that will act as the foundation for good business practices and adequate consumer safeguards. To this end, there is a need for capacity building, mutual learning, evolution of appropriate regulation and sharing of best practices. It was suggested that this should be addressed during this cycle under ‘Question 6/1 deliverables’, which could include guidelines, toolkits and best practices.

Document [SG1RGQ/35 \(Proge-Software, Italy - SME pilot participant\)](#) shares information about its model used to support the Italian Government and private companies to achieve GDPR and AgID¹²⁶ compliance. It suggests that such proposals could be included as a possible example to define guidelines for governments and private companies for the Data Privacy Regulations Compliance Process. Participants remarked that the document touches on the core issues of the Question and could therefore be considered to be included as information in the report. Countries could contribute information on how they are dealing with the cloud, in particular to protect consumers using cloud service platforms. Participants also said that many SMEs face challenges, and guidelines and best practices could be useful.

Document [SG1RGQ/38 \(Haiti\)](#) contains initial text to be considered for Chapter 1 of the report.

Document [SG1RGQ/72 \(Zimbabwe\)](#) highlights telecommunication consumer needs from the perspective of Zimbabwe’s mobile telecommunication service providers and consumer watchdogs. The contribution examines access needs, especially in rural and remote areas, as well as social and economic needs of telecommunication consumers in Zimbabwe. The input was provided in response to a circular sent to the major mobile telecommunication operators and the main consumer watchdogs in Zimbabwe. Consumers and service providers are targeted in the questionnaire in order to have a full picture of consumer needs as well as that of the service providers. E-education, e-agriculture, mobile banking and e-health featured repeatedly in the feedback received. In response to an enquiry from participants, the delegate from Zimbabwe explained that an additional survey should be carried out to specifically identify consumer needs of persons with disabilities.

[Document SG1RGQ/96. \(Islamic Republic of Iran\)](#) from **Iran University of Science Technology (IUST)** proposes that the Question should also address child protection in the online environment, including by listing possible actions in terms of government/NGOs as well as for parents. The

¹²⁶ *Agencia per l’Italia Digitale (AgID)*. [About us](#).

contribution includes conclusions from a research project carried out by the Research Centre for ICT Strategic and International Studies at IUST.

Document [SG1RGQ/56 + Annex](#) (**BDT Focal Point for Q6/1**) contains the GSR-18 Best-Practice Guidelines that address the potential of emerging technologies, business and investment models as well as policy and regulatory approaches for continued innovation. It also contains concrete recommendations for regulators to consider in approaching the new regulatory frontiers. Participants also suggested that WSIS documents and the Council Working Group on the Internet could be useful for ITU-D study group Questions.

Document [SG1RGQ/57 + Annex](#) (**BDT Focal Point for Q6/1**) presents a quantitative analysis of data collected by ITU on International Mobile Roaming (IMR) regulatory and policy strategies as well as a brief introduction to the future of IMR, in particular on roaming for Internet of Things (IoT) and machine-to-machine (M2M) communications.

Document [SG1RGQ/58](#) (**BDT Focal Point for Q6/1**) provides information from the ITU-D regulatory survey, focusing in particular on consumer-protection issues.

Document [SG1RGQ/66 + Annex](#) (**BDT Focal Point for Europe**), containing the report on the outcomes of a workshop on the future of cable TV held in January 2018, indicated that information from the workshop may be considered for the report.

Document [SG1RGQ/TD/5](#) (**Guinea**) provides information on telecommunication market development in Guinea and calls on the group to provide best practices, guidelines and tools to assist countries, in particular developing countries, in their digital transformation relating to consumer-awareness and consumer-protection issues. Participants contributed by giving examples of how they raise awareness in their respective countries.

Liaison statements: Documents [SG1RGQ/ADM/2](#) (list of liaison statements), [SG1RGQ/1](#) (BDT), [SG1RGQ/10](#) (ITU-T Study Group 2) and [SG1RGQ/22 + Annex](#) (ITU-T Study Group 11).

Document [SG1RGQ/84](#) (ATDI, **France**) provides a mapping of ITU-D SG1 and SG2 Questions to ITU-R Working Parties. Question 6/1 is only mapped to ITU-R WP1B, which relates to regulators and covers issues such as licences that are relevant to consumers. Participants said they would be interested in discussing with the group that deals with cross-border coordination issues. They were assured that this could be addressed in WP1B.

Document [1/104](#) (**TRA, Oman**) focuses on a campaign created at the initiative of the TRA to promote awareness on electronic scams.

Document [1/111](#) (**Papua New Guinea**) addresses the efforts undertaken by the National ICT Authority of Papua New Guinea to promote consumer protection and welfare through the Consumer Protection Rule, 2014. Several participants added that their respective countries have adopted similar laws. They highlighted the importance of such legal frameworks as well as adherence to the rules to safeguard the interests of consumers. Kuwait shared its guidelines on consumer protection, which is available in Arabic.

Document [1/134](#) (**Benin**) provides information on Benin ARCEP's new automated web-based platform for the management of consumer complaints regarding electronic communication and postal services.

Document [1/179](#) (**Benin**) highlights the importance of the role of regulatory authorities in dispute resolution and illustrates how the NRA in Benin has strengthened its capacity for institutional mediation for the protection of consumers.

Document [1/153](#) (**State of Palestine**, which participates in ITU work under Resolution 99 (Rev. Dubai, 2018) of the Plenipotentiary Conference) focuses on various awareness-raising campaigns organized by the Ministry to provide consumers with better ICT services.

Document [1/154](#) (**Central African Republic**) describes the current situation with respect to ICT consumer protection in the Central African Republic. The chairman agreed that this contribution could enrich the report in various chapters.

Document [1/174](#) (**Rapporteur for Q4/1**) reports on the ITU-D Study Group 1 Experts' Knowledge Exchange session on Question 4/1 and Question 6/1, which was held back-to-back with the ITU Regional Economic Dialogue on Telecommunications/ICTs for Africa (RED-AFR) in Ouagadougou, Burkina Faso, 8-9 October 2018, to collect regional experiences and explore new ways of building synergies between the work that is taking place in the region and the activities that are currently under way in the ITU-D study groups.

Document [1/186](#) (**Mexico**) provides information from the Federal Telecommunications Institute (IFT) of Mexico on '*Surveys to Users of Telecommunications Services*'.

Document [1/187](#) (**Mexico**) provides information on '*Telecommunications Users Satisfaction indicators Methodology*' to help the different sectors, regulated agents, researchers and anyone interested in the analysis of the sector with analysis and/or decision-making.

Document [1/188](#) (**Mexico**) highlights reports published by IFT on '*Comparable Information of Plans and Rates for Telecommunications Services*' and '*Plans and Rates Evolution*' in order to help reduce information asymmetries and to promote the empowerment of users.

Document [1/189](#) (**Mexico**) presents guidelines published in January 2018 that set the indices and quality parameters for mobile service providers to adhere to.

Document [1/194](#) (**Mexico**) focuses on results of a survey and advice IFT has issued on its website on cybersecurity in the use of fixed and/or mobile Internet, including on how to install and update antivirus software, change passwords, back up information regularly and connect to secure public networks.

Document [1/198](#) (**India**) indicates that as regulation catches up with technological change, regulatory loopholes can be exploited to the detriment of consumers and competitive market conditions, and proposes that regulators should strive to understand, cooperate and coordinate to implement protective and corrective measures. While appreciating the contribution, participants at the meeting called upon the team to ensure consistency with ITU-R recommendations and other ITU definitions in terminology. Some participants also raised concerns with some of the substantive assertions related to big data and digital platforms.

Document [1/219](#) (**Brazil**) illustrates its experience on the regulation of customer care. Following adoption of the Consumer Defence Code and an executive decree concerning adequate customer care, Anatel has been enforcing operators' performance based on both qualitative requirements and procedural indicators.

Document [1/220 \(China\)](#) highlights China's experience in the protection of consumer rights and interests where a government-led and multistakeholder supervision and protection system was established. The document also recommends that given the constant and rapid market developments, industry supervision and the protection system should be continuously improved in order to effectively protect the legitimate rights and interests of users.

Document [1/248 \(Zimbabwe\)](#) provides information on the development and consolidation of consumer laws in Zimbabwe and the public hearings and consultations on Zimbabwe's Consumer Bill. The bill highlights basic consumer rights and proposes enforcement measures. The contribution also makes a number of recommendations for wider application, including the promulgation of sector-specific regulations. Zimbabwe requested feedback on the provisions of the bill.

ITU-T Study Group 2 Documents [1/TD/16](#) on *ClickFarms* and [1/TD/18](#) on *Countering and combating the absence of Calling Line Identity (CLI)* and administrative documents - Documents [1/ADM/21](#), which lists Q6/1 documents, and [1/252](#), which shares information and lessons learned as indicated by members in their contributions to the SG1 meeting) - were noted. While appreciating the level of contributions, the Rapporteur encouraged participants to continue to contribute their experiences relevant to this Question so as to enrich the report.

Document [SG1RGQ/143 \(Haiti\)](#) (case study) describes the work undertaken by the Haitian Administration as well as challenges faced and possible solutions in the light of concerns from consumer associations and individual consumers. The Vice-Rapporteur from Haiti, Mr Altemar, provided further details and clarification on the case study, in particular on the setting up of the unit, the role and mandate of the unit and the regulator on consumer protection, sanctions and enforcement, mechanisms and processes, solutions to issues reported, channels to communicate with the regulator, and the role of consumer associations.

Document [SG1RGQ/151 \(India\)](#) presents issues and solutions, shares examples of collaboration, and makes recommendations for regulators to sustain trust and ensure consumer protection in the use of digital communication services, including the need for collaborative regulation. The Vice-Rapporteur Ms A. Gulati from India, also highlighted the need for capacity building and sharing of materials and experiences through the creation of a repository of materials. Participants requested further information on the strategy adopted by the Indian Administration to achieve such collaboration with market players and technology companies. Others requested information on how competition rules (draft policy) can be applied to online retail platforms not based in India.

Document [SG1RGQ/153 + Annex \(BDT Focal Point for Q6/1\)](#) presents a 2019 GSR Discussion Paper - *Building confidence in a data-driven economy by assuring consumer redress*. The document addresses issues related to consumer protection in a digital age and could provide useful background for several chapters that contribute to guidelines and principles to be considered by the rapporteur group.

Document [SG1RGQ/155 \(State of Palestine\)](#) (case study) shares information on campaigns organized by the ICT Ministry to inform consumers about promotional campaigns run by mobile-telephone companies and the fixed-service company in the State of Palestine.

Document [SG1RGQ/162 \(State of Palestine\)](#) (case study) sets forth proposed instructions on the provision of telecommunication services and promotional campaigns and offers, based on Articles 28(e) and 6(e/f/g) of the Palestinian Telecommunications Act. The instructions will

be subject to annual review in the light of experience gained from the development of the telecommunication market and any changes to the Act or relevant legislation.

Document [SG1RGQ/169 \(Benin\)](#) (case study) highlights several regulatory measures taken by Benin's Regulatory Authority for Electronic Communications and Post (ARCEP) in order to facilitate the establishment of radio facilities in conditions that guarantee the safety of users and operating staff of electronic communication networks as well as the protection of the environment, while respecting constraints associated with urban and regional planning throughout the Republic of Benin. It also focuses on difficulties encountered during installation, in particular public opposition to the installation, or calls for the dismantling of facilities, and invites other Member States to share their experiences.

Document [SG1RGQ/170 \(Comoros\)](#) (case study) shares information on the development of the ICT/telecommunication market in the Comoros as well as its legal and regulatory framework, highlighting that the limitation of the legal framework limits the ability of the regulator to assist consumers.

Document [SG1RGQ/171 \(Democratic Republic of the Congo\)](#) (case study) notes the development of the ICT/telecommunication market in the Democratic Republic of the Congo as well as its legal and regulatory framework.

Document [SG1RGQ/172 \(Burkina Faso\)](#) (case study) mentions the new regulations adopted in December 2018 on ways of identifying electronic communication service subscribers and cybercafé customers. The new regulatory framework is intended to help prevent ICT services being used for criminal purposes and to protect ICT consumers.

[SG1RGQ/178 \(Burkina Faso\)](#) (case study) on the regulatory process for the adoption of the Digital Planning Roadmap in Burkina Faso. The roadmap provides a reference document for digital planning and implementation in Burkina Faso. It provides a practical and operational planning tool as well as the legal basis that will help reduce the country's digital divide in terms of access to high-speed and very high-speed broadband by 2030.

Document [SG1RGQ/174 \(India\)](#) (case study), addresses unsolicited commercial communications (UCC) and explains the framework adopted by India to curb UCC by way of regulation in cooperation with telecom service providers (TSPs).

Document [SG1RGQ/182 \(TRAI, India\)](#) discusses the approach for testing broadband speed and the working of the 'TRAI My Speed' app, an analytic portal to judge the speed of broadband services being provided by TSPs. Such initiatives are aimed at allowing consumers to make an informed choice about the level of services made available by their TSPs, for regulators and policy-makers to assess the quality of services being provided by TSPs, and for governmental insight on the extent and level of achievement of goals set by them.

Document [SG1RGQ/191 \(Guinea\)](#) presents an overview of the ICT/telecommunication market and relevant legal and regulatory framework in Guinea. It highlights legislation passed in 2016 of particular importance to consumers, including an act on cybersecurity and personal data protection and an act on electronic transactions. A personal data protection commission is being set up. It further affirms that, in addition to a legal framework, awareness and education in using information technologies, data protection and management, it is necessary to follow up on problems and consumer complaints. This should be made a priority so as to ensure better

protection for consumers. Capacity building and sharing of experiences can help strengthen skills of professional stakeholders and address challenges related to the digital world.

Document [SG1RGQ/201](#) (**Russian Federation**) highlights best practices of the Russian Federation in establishing a quality-of-service system for telecommunications/ICTs and its activities to protect the key interests of communication service consumers, thereby helping to put providers and consumers of communication/ICT services on an equal footing in their relations.

Document [SG1RGQ/206](#) (Brazil) shares a case study from Brazil focusing on the regulatory and institutional approach of Anatel to unsolicited calls (abusive calls) and telemarketing to enforce consumer protection and rights.

Document [SG1RGQ/215](#) (**Brazil**) provides information and a general overview of the terms of the recently enacted Brazilian Personal Data Protection Law. It includes the background, object and scope, the concept and types of personal and processing data, as well as the principles, the agents involved, the legal permissions for domestic and international processing, the basic rights of data subjects, and the creation of the data-protection authority in Brazil.

Document [SG1RGQ/232 + Annex](#) (**BDT Focal Point for Europe**) includes a summary of actions of the ITU Office for Europe for 2019. It provides key outcomes, where possible, for actions already implemented as well as relevant weblinks to outcome reports and to event webpages. It summarizes upcoming actions for 2019 and also lists the 2019 training status of the ITU Europe network of centres of excellence (CoE). In annex, information on all events of 2019 and a list of planned events for 2020 are provided. All actions are grouped under the five regional initiatives for the Europe region agreed at WTDC-17.

Document [SG1RGQ/241](#) (**Zimbabwe**) highlights the link between satisfaction of consumer needs and access to broadband. It concludes that investment, solutions to the digital divide, research and innovation are key elements for broadband roll-out and affordability of broadband access. It recommends resolution of the problems related to these key elements in order to improve broadband coverage, broadband adoption and consumer satisfaction. There is also a need to ensure coordination with Question 5/1 and avoid overlap.

Document [SG1RGQ/244](#) (**Ghana**) focuses on protection against unfair market practices. As an example, it highlights the introduction of the Billing Feedback Message (BFM) in Ghana in 2013 that was aimed at reducing complaints on billing, ensuring transparency on billing, and addressing issues of perceived wrongful charges on network services. In order to address the challenge of service providers taking advantage of the system and using the same platform for advertisement, Ghana introduced measures to protect consumers against unfair market practices on billing in the telecommunications market as well as mechanisms to guarantee adequate transparency and consumer protection.

[Document SG1RGQ/259](#) (**BDT**) shares information on lessons learned as indicated by members in their contributions to the second block of ITU-D SG1 Rapporteur Group meetings for the 2018-2021 study period. The document includes a list of extracted lessons learned that are relevant for Q6/1. BDT also presented Document [SG1RGQ/258](#) that elaborates on collaboration opportunities with ITU-D study groups and the WSIS platform, including the potential reuse of ICT-related activities reported in the WSIS Stocktaking Database as well as potential participation and contribution by WSIS participants in ITU-D study groups. Some possible next steps are also provided for consideration, which include identification by the ITU-D rapporteur groups of

WSIS documents relevant to their Question and collaboration with their authors, along with the possibility of organizing an ITU-D study group-related session during WSIS Forum 2020.

Liaison statements: Document [1/ADM/20](#) contains a list of incoming liaison statements.

Document [1/307](#) (**India**) cites the example of the National Institute for Transforming India (NITI Aayog) that has published a discussion paper titled 'AI for All', laying the ground for the National Strategy on Artificial Intelligence and building capacity on these issues. The contribution highlights the unique challenges emanating from the use of AI in digital services, indicating that this requires

1. Appropriate institutional mechanisms within Member States that would keep abreast of latest technologies and advise on cross-sectoral legislation and regulation, including areas of consumer awareness and protection.
2. The need for international consensus and cooperation on standards, ethics and consumer protection. Among the recommended best practices is for governments to develop an AI national plan to outline key strategies for preparing the country for AI.

Document [1/317](#) (**Russian Federation**) provides a case study and contains information on the experience of the Russian Federation in abolishing national and online roaming charges in the country. The contribution refers to recently adopted regulations related to roaming-at-home. Participants suggested that the information could be integrated into the Question 6/1 final report (Chapter 1, section 1.1; Chapter 3, section 3.4; and Chapter 4) and in the annex.

Document [1/328](#) (**United Kingdom**) identifies how numbering misuse could impact consumers, both directly and indirectly. Examples of these types of misuse are presented together with some initial means to overcome or minimize such impacts. The contribution also highlights that such tools should not be seen in isolation but rather used in conjunction with the tools that are deployed by administrations or regulators at points of interconnect, both national and international. It was suggested that the information could be included in sections 1.3.5 and 4.3.4 and that the results of the survey during the previous period could also provide useful information and should be included in the Question 6/1 final report.

Document [1/329](#) (**Papua New Guinea**) provides a case study with a proposed regulatory framework for QoS. The "draft Rule on Telecommunication Quality of Service Performance Monitoring", which is the subject of a public consultation, seeks to establish a performance measurement and monitoring regime with respect to retail telecommunication services, including mobile-telephony, fixed-broadband and mobile-broadband services that are popular with retail subscribers. Amongst other things, NICTA envisages that, over time, this information, when presented in a meaningful format, will enable consumers to better understand and compare the quality of services between different service providers whilst also providing an incentive to licensees or service providers to improve their performance.

Document [1/334](#) (**India**) provides a case study describing TRAI's Telecom Commercial Communications Customer Preference Regulation that combines co-regulation with new technology (blockchain) to try and curb the menace of unsolicited commercial communications (UCC). Telecommunication service providers will establish and arrange the framework for compliance with the necessary flexibility and speed required to combat spammers who continually change their tactics and morph their identities to escape detection. The framework is user-friendly and automated using technological advancements to smooth the processes and to reduce the cost of compliance.

Document [1/336 \(Zimbabwe\)](#) provides an overview of consumer legislation with relevant references from various countries (through contributions and research). It covers legislation on consumer rights as well as other legislation and regulations to protect consumers. It also highlights the need for the development of legal frameworks in relation to AI and IoT.

Document [1/344 \(India\)](#), a case study from India, addresses regulatory questions related to online platforms in terms of consumer protection and competition. The Indian approach is a mix of encouraging self-regulation and filling gaps with State regulation. The contribution points to a study by India's competition regulator that looks at platform neutrality (third-party treatment versus own products and services), transparency (of search results and reviews) and data-sharing practices, and calls for greater transparency of platform practices in these areas to address information asymmetry and competition concerns. The study concludes with recommendations on self-regulatory measures that platforms are encouraged to implement in the area of greater transparency and disclosure on:

- i. search ranking;
- ii. collection, use and sharing of data;
- iii. user review and rating mechanism as well as contract terms and discount policies *vis-à-vis* sellers.

Document [1/349 \(Mexico\)](#) is a case study on the Digital Literacy Programme "*Conoce tus derechos*" that provides an information mechanism for IFT Mexico to accomplish direct communications with users through general training and provision of informational material. The aim of the programme is to empower users of telecommunication services with information that allows them to demand their rights as users, using tools that the Institute has developed in their favour to make informed decisions, and to use their telecommunication services and equipment appropriately.

Document [1/353 \(State of Palestine\)](#) provides an overview of the law addressing offers of both the non-competitive and competitive telecommunication services, specifying the rights and obligations, including those regarding telecommunication devices, mobile Internet, offers of the general fixed-telecommunication companies, duration of the offers, and consequences of contravention of the instructions. This will be an important input to Chapter 4, participants concluded.

Document [1/374 \(Rev.1\) \(TRA, Oman\)](#) is a case study from TRA to review the mechanism for providing services to advertising companies, the method of sending bulk SMS to users and the method of unsubscribing from receiving promotional SMS. The method for unsubscribing was assessed in terms of its effectiveness and its availability to beneficiaries free of charge - and to the extent the systems of telecommunication companies can be modified to allow the flow of promotional messages based on a request from beneficiaries to opt-in to this service rather than making opting-out necessary to stop the service. The telecommunication companies were requested to provide copies of the contracts concluded between them and the companies promoting their services and products.

Document [1/397 \(KDDI Corporation, Japan\)](#) shares information on how KDDI Corporation is promoting initiatives of "smartphone safety classes" under the corporate philosophy to "achieve a truly connected society". The company sends certified lecturers to primary, secondary and high schools all over Japan and holds "smartphone safety classes" to have students learn rules and manners and not to get into trouble.

Document [SG1RGQ/307 \(State of Palestine\)](#) set out measures taken to review subscription services and update subscription contracts to respond to challenges from the global pandemic. The contribution also illustrates how the Complaints and Consumer Protection Unit can proactively manage the issue and work to guarantee the accessibility, quality and affordability of subscription services.

Document [SG1RGQ/309 \(Brazil\)](#) shared the results achieved by Anatel in the strategy of migrating from traditional helpdesk call centres to digital services channels under customer care service. The report also presented the history of the use of the channels and the continuity of this strategy.

Document [SG1RGQ/310 \(Brazil\)](#) presented a brief study illustrating how innovation and digitalization applied to customer care in the telecommunication sector can combine human interaction and technology in order to provide more meaningful interactions to the consumer, reduce time and effort, and improve customer experience and satisfaction. In Brazil, where consumers' interactions through traditional channels, mainly by phone, take a lot of time and effort, it is especially demanded of telecommunication companies to focus on reducing the time-effort duo and on improving customer experience and satisfaction, regardless of the contact channel used by the consumer.

Document [SG1RGQ/311\(Rev.1\) \(Brazil\)](#) looks at how communication between consumers and service providers has changed over time. It highlights examples in selected countries with potential lessons to be learned based on data collected in close collaboration with Cullen International, a leading regulatory intelligence analyst that provides unbiased information covering telecommunications, media, digital economy and competition law trusted by over 270 industry players and regulators worldwide.

Document [SG1RGQ/360 \(Brazil\)](#) reaffirmed that in response to emergencies, one of the roles of the Brazilian National Telecommunications Agency (Anatel) is to keep Brazilians connected, especially during the present pandemic. It is an unprecedented challenge and, in Anatel's view, solutions will depend on a variety of arrangements as there is no unique formula to handle the complexity of the current situation. The Agency follows measures developed by the service providers and discusses with them as well as with other bodies, local governments and civil society in search of solutions that will address the legitimate concerns of all.

Document [SG1RGQ/358 \(India\)](#) provides an overview of the evolution of regulations in India and the present regulatory framework adopted by India to curb unsolicited commercial communications (UCC) - communications made through telecommunication services by message, voice or SMS and transmitted to subscribers without their consent or willingness. These could be for the purpose of informing, soliciting or promoting any commercial transaction in relation to goods, investments or services, but does not include any transactional message or service messages, nor any messages transmitted by or on the directions of the State or competent authority. Apart from being a source of inconvenience, such communications also impinge upon the privacy of individuals.

Document [SG1RGQ/326 \(Zimbabwe\)](#) provided information on how consumer needs have changed during the period that the world has been facing the COVID-19 pandemic. It indicated that the COVID-19 pandemic has shown how regulators and policy-makers need to go back to the drawing board and come up with policies that encourage investment in rural and remote areas, especially for last mile connectivity. It suggests that solutions that connect individual

homes become a priority for rural and remote areas to ensure that consumers continue to have access to ICTs particularly during pandemics.

Document [SG1RGQ/342 \(Ghana\)](#) provided an overview of the Billing Verification System (BVS) that verifies prices charged by the mobile network operators (MNOs) and ensures that tariffs are fair and reasonable and do not discriminate unduly among consumers. It aims to ensure consumers are adequately protected against unfair marketing practices, as tariffs are essential to the mandate of the telecommunication regulator in Ghana. The billing feedback messaging feature was introduced to Ghanaians to ensure transparency on billing and to empower consumers to track their activities on their usage of telecommunication services.

Document [SG1RGQ/TD/17 \(Nigeria\)](#) shed light on the response to the menace of unsolicited telemarketing messages in the Nigerian telecommunication industry by the regulatory instrument introduced in Nigeria.

Document [SG1RGQ/373 \(BDT Focal point for Q1/1, Q3/1, Q4/1, Q6/1\)](#) introduced the Digital Regulation Handbook and Online Platform, the result of an ongoing collaboration over two decades between ITU and the World Bank. It aims to provide practical guidance and best practices for policy-makers and regulators across the globe concerned with harnessing the benefits of the digital economy and society for their citizens and firms.

Document [SG1RGQ/374 \(BDT Focal point for Q1/1, Q3/1, Q4/1, Q6/1\)](#) presented the GSR-20 Best Practice Guidelines. According to the guidelines, the COVID-19 pandemic has revealed that connectivity for all is essential for economic activity and citizen welfare, and that key digital challenges cannot be overcome by one stakeholder group alone. Within this context, the guidelines conclude that in order for the digital economy to grow sustainably and to ensure service and business continuity, including in times of crisis, regulators and policy-makers need to find an appropriate balance between facilitative actions to promote digital transformation and affordable connectivity. While ensuring long-term social policy objectives are met, an adaptive, resilient, collaborative and fit-for-purpose regulatory ecosystem is necessary for open and competitive digital markets to thrive along with delivering positive consumer outcomes and providing the foundation for digital transformation. Inputs from this contribution will be reflected in Chapter 2.5 with a reference to the publication.

Annex 2: Outcomes of the ITU Global Symposium for Regulators in 2018 and 2019 (GSR-18 and GSR-19)

2018 Global Symposium for Regulators (GSR-18) (Geneva, Switzerland, 9-12 July 2018)

Digitalization is increasingly and fundamentally changing societies and economies and disrupting many sectors in what has been termed the 4th Industrial Revolution. Meanwhile, ICT regulation has evolved globally over the past 10 years and has experienced steady transformation. As regulators, we need to keep pace with advances in technology, address the new regulatory frontiers and create the foundation upon which digital transformation can achieve its full potential. Being prepared for digital transformation and emerging technologies, such as AI, IoT, M2M and 5G is fundamental. We, the regulators participating in the 2018 Global Symposium for Regulators, recognize that flexible and innovative policy and regulatory approaches can support and incentivize digital transformation. The best practices in this regard would allow us to respond to the changing landscape and address the continuing need for secure and reliable ICT infrastructure, affordable access to and delivery of digital services, as well as protect consumers and maintain trust in ICTs. We have therefore identified and endorsed the following regulatory best-practice guidelines on new regulatory frontiers to achieve digital transformation:

- I. Fostering the potential of emerging technologies for digital transformation.
- II. Business and investment models to support digital.
- III. Policy and regulatory approaches for continued innovation and progress transformation.

To this end, regulators participating in the 2018 Global Symposium for Regulators, declared that they need to:

- Consider putting in place innovative, out-of-the-box measures, such as regulatory sandboxes for enterprises wishing to test an emerging technology or innovative service without being bound by all the regulations that would normally apply.
- “Start-up and experiment” interfaces to support start-ups, enterprises and communities in their experimental initiatives.
- 5G pilot projects to obtain initial feedback and facilitate reflection and design of future spectrum allocations while stimulating the take-up of services, building specific use cases and assessing future challenges related to emerging technologies under real-life conditions.
- Promote further public participation and consultation in the regulatory process through regulation by data that is based on information and the observations of digital stakeholders and users to provide citizens and stakeholders with the most detailed and transparent information, and allowing consultation and participation in the regulatory decision-making process to complement the regulators’ traditional tools.
- Establish effective mechanisms for cooperation across the sectors, including with consumer protection authorities, service providers and other relevant bodies at the national, regional and international levels, to promote the development of cross-cutting services, such as e-commerce, e-banking and e-health.
- Consider, as appropriate and within our mandate, the necessary frameworks to ensure privacy and security of government, business and consumer data so that stakeholders are adequately informed about potential security and privacy challenges they may face with online services, and have access to timely and accurate information regarding the services and applications they use (including reliability, speed, quality of service and data traffic management).

2019 Global Symposium for Regulators (GSR-19) (Port Vila, Vanuatu, 9-12 July 2019)

Technology paradigms and business models challenge existing regulatory patterns and frameworks. From the imminent entry in markets of 5G and IoT, to the profusion of cloud services and AI, regulatory response requires a new perspective. Unleashing the full potential of digital will require an actionable, agile, collaborative, innovative and outcome-based approach to regulation. In the increasingly complex and dynamic digital transformation, it is important to agree on common principles and put forward clear and simple rules – and follow them forward.

In this regard, regulators participating in the 2019 Global Symposium for Regulators recognize that there is no single, comprehensive blueprint for best practice and that regulatory patterns for the digital transformation will be rooted in local circumstances while addressing regional and global challenges. They nevertheless agreed that country experiences can be enlightening and guide them towards regulatory excellence for the benefit of all.

They identified and endorsed these regulatory best-practice guidelines to fast-forward digital connectivity for all to allow everyone to participate in the digital economy and benefit from digital transformation. Recalling the series of GSR Best Practice Guidelines since 2003 that capture established regulatory wisdom and tried-and-tested practices, the focus of the regulators is on new and innovative approaches, tools and mechanisms for achieving inclusive digital infrastructure and services.

1. Core design principles for collaborative regulation

- i. *To achieve digital transformation, policy and regulation should be more holistic.* Cross-sectoral collaboration along with revisited regulatory approaches, such as co-regulation and self-regulation, can lead to new forms of collaborative regulation based on common goals, including social and economic good, and innovation.
- ii. *Policy and regulation should be based on consultation and collaboration.* In the same way that digital cuts across economic sectors, markets and geographies, regulatory decision-making should include the expectations, ideas and expertise of all market stakeholders and players, including academia, civil society, consumer associations, data scientists, end users and relevant government agencies from different sectors.
- iii. *Policy and regulation should be evidence-based.* Evidence is critical for creating a sound understanding of the issues at stake and identifying the options going forward as well as their impact. Appropriate authoritative benchmarks and metrics can guide regulators in rule-making and enforcement, enhancing the quality of regulatory decisions.
- iv. *Policy and regulation should be outcome-based:* Regulators need to address the most pressing issues, for example market barriers and enabling synergies. The rationale for any regulatory response to new technologies should be grounded in the impact on consumers, societies, market players and investment flows as well as on national development as a whole.
- v. *Policy and regulation should be incentive-based.* Collaborative regulation is driven by leadership, incentive and reward. Regulators should keep a wide array of investment incentives at hand to provide impetus for markets to innovate and transform while maximizing benefits to consumers.
- vi. *Policy and regulation should be adaptive, balanced and fit for purpose.* Regulation-making is about flexibility – continually improving, refining and adjusting regulatory practices. The balance in regulatory treatment of new services is more delicate than ever. A close, continuous link to markets and consumers is important to get digital on the right glidepath to achieving social and economic goals.
- vii. *Policy and regulation should focus on building trust and engagement.* Collaborative regulation provides the space for co-creating win-win propositions, working towards

regulatory objectives while increasing the engagement of industry. Trust becomes the foundation of the regulatory process, underpinning the growth of digital.

2. Benchmarks for regulatory excellence and market performance

We recommend five main clusters of benchmarks for regulators:

- i. *Connectivity mapping*: Tracking the deployment of the various kinds of digital infrastructure can inform the regulatory process and allow regulators to identify market gaps and market stakeholders – and turn them into opportunities for investment and growth.
- ii. *Metrics for market performance*: Metrics allow regulators to assess the performance of market segments for digital services against social and economic goals and identify priority action areas for policy and regulation.
- iii. *Measuring regulatory maturity and levels of collaborative regulation*: Regulatory benchmarks pinpoint the status of advancement of policy and regulatory frameworks for digital markets. They help track progress and identify trends and gaps in regulatory frameworks, making the case for further regulatory reform towards achieving vibrant and inclusive digital industries.
- iv. *Impact assessment*: A combination of quantitative and qualitative econometric studies based on reliable data can enable regulators to explore, understand and quantify how digital technologies, market players or regulation can contribute economically to growing the larger digital ecosystem and making it more inclusive.
- v. *Regulatory roadmaps* based on established authoritative metrics can guide regulators towards achieving digital connectivity objectives in a faster and better-targeted way. In order to leverage these evidence-based instruments, the volume and quality of data accessible to regulators need to be increased, and their sources diversified. These instruments can also enable market players to reflect on their performance and impact on the economy and development, and on how they can engage in self-regulation.

3. What regulatory tools and approaches are at hand for enabling digital experimentation?

We recognize that, among the many tools that can improve digital market outcomes, the following form the core of collaborative regulation best practice:

- Space for digital experimentation: From temporary licences and new technology pilots to regulatory sandboxes, a range of tools and techniques can be used to create a dynamic regulatory environment in which digital market failures and opportunities have space and flexibility to address present and future challenges. Such methodologies can also be employed to design strategies to enhance digital applications and skills.
- Pro-competition frameworks for the digital transformation should consider longer value chains, more diverse market players, services and devices, stakeholder partnerships and digital infrastructure layers and, ultimately, their impact on markets, consumers and Internet neutrality. Nonetheless, excessive and unwieldy regulation must be avoided.
- Regulatory incentives can create a positive market dynamic and improve market outcomes with less regulatory effort.
- Stakeholder engagement vehicles, such as public hearings, high-level roundtables, expert workshops and hackathons can allow pooling of resources and expertise to inform major regulatory decisions.
- Robust and enforceable mechanisms for consumer protection, including a set of rules on data protection, privacy and data portability as well as accessible mechanisms for consumer redress are essential to support digital transformation in economic sectors across the board and ensure consumers' interests are safeguarded.

- Market-based and dynamic mechanisms for spectrum management can allow for flexible, simplified and transparent use of scarce radio frequencies, while promoting technology neutrality.
- Regulatory Impact Assessment (RIA): Enhanced with new benchmarks and data analysis, RIA allows for better decision-making and should be introduced as a regular practice before major regulatory decisions are made as well as throughout the lifecycle of regulation.
- Agile data-driven monitoring solutions, based on standards for the interoperability of data systems and tools among regulators and market players, can facilitate market oversight in areas such as quality of service and experience as well as regulatory compliance.
- Diversified mechanisms for consumer engagement and feedback multiply regulatory inputs and allow for fine-tuning regulatory policies and their implementation.
- Effective channels for dynamic collaboration among regulatory authorities, such as the ICT, financial and competition authorities as well as law-enforcement agencies and the judiciary, are necessary to ensure coherent and reasonable regulations across economic sectors. Regulatory sandboxes involving multiple regulators can incubate key cross-sector regulations, such as for digital financial inclusion.
- Regional and international cooperation in defining regulatory rules on cross-border issues can ensure consistency, predictability and fluidity of digital markets and will catalyse the deployment of region-wide and global digital infrastructure, from fibre backbones and submarine cables to mobile networks and satellite connectivity.
- Regulatory expertise needs to be developed continuously to integrate new technologies, competencies and skills, and allow for data and evidence-based decision-making.

The GSR-19 discussion paper on *"Building confidence in a data-driven economy by assuring consumer redress"* includes examples of best practice and makes recommendations to improve effectiveness, covering such areas as:

- Collaborative development of consumer-protection policies, regulation and mechanisms across the sector: media, ICT, competition, as well as products and services.
- Collaboration between different policy-making ministries, such as those responsible for utilities, finance and business, education, health, agriculture and tourism.
- Collaboration between policy-makers and regulators; different regulators; regulators and industry; and regulators and consumer associations.
- Consumer complaint handling and empowerment initiatives and mechanisms in policies, laws and regulations to foster more effective consumer complaint handling mechanisms with the industry.
- Impact of cross-border activities.

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdttdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Digital Networks and Society (DNS)

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: +237 22 22 9292
Tel.: +237 22 22 9291
Fax: +237 22 22 9297

Senegal

Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3^e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10^o andar, Ala Sul
(Anatel)
CEP 70070-940 Brasília - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt

International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand

International Telecommunication Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication Union (ITU) Area Office
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation

International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: euregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-34621-8



9 789261 346218

Published in Switzerland
Geneva, 2021