INTERNET & JURISDICTION

GLOBAL STATUS REPORT 2019

AUTHOR: PROF. DAN JERKER B. SVANTESSON

INTERNET & JURISDICTION POLICY NETWORK

This Report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network and authored by Professor Dr. Dan Jerker B. Svantesson.

The Internet & Jurisdiction Global Status Report 2019, 1st Edition, is published by the Secretariat of the Internet & Jurisdiction Policy Network.

The author of this Report made a best effort to map the current ecosystem and trends based on desk-research, as well as stakeholder surveys and interviews. The completeness of information can however not be guaranteed, as this Report constitutes a first global baseline on the state of jurisdiction on the internet. Moreover, the analysis of the author does not necessarily reflect the view of the Secretariat of the Internet & Jurisdiction Policy Network, of stakeholders engaged in the Internet & Jurisdiction Policy Network, or of the financial supporters of the Report.

Internet & Jurisdiction Policy Network - Paris, France

The Secretariat of the Internet & Jurisdiction Policy Network is grateful for the financial and institutional support of the following entities that have enabled the production of the Report:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

On behalf of Federal Ministry for Economic Cooperation and Development

Republic of Estonia Ministry of Foreign Affairs

European Commission

REPORT CITATION

Internet & Jurisdiction Policy Network (2019). Internet & Jurisdiction Global Status Report 2019.

FOREWORDS

BERTRAND DE LA CHAPELLE and PAUL FEHLINGER
Executive Director and Deputy Executive Director
Internet & Jurisdiction Policy Network

How to handle the coexistence of heterogeneous laws on the cross-border internet is one of the greatest policy challenges of the digital 21st century. Yet, scalable and coherent policy solutions cannot be developed without a comprehensive understanding of a highly complex and dynamic ecosystem comprised of multiple actors, initiatives and trends across the policy silos of digital economy, human rights and security. This was a clear call by over 200 key stakeholders from 40 countries at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in 2018. However, even decades after the rise of the commercial internet, such consolidated data did not yet exist. To provide this indispensable mapping and analysis, the Secretariat of the Internet & Jurisdiction Policy Network decided to launch the world's first Internet & Jurisdiction Global Status Report.

Drawing on the unique expertise of key stakeholders engaged in the policy development work in the Internet & Jurisdiction Policy Network, this inaugural edition of the Global Status Report provides a first snapshot and baseline. This Report should be understood as a foundational dataset that will allow us to collectively proceed and fill in the gaps in future global and regional editions. For this ambitious and crucial endeavour, we invite all stakeholders to contribute their knowledge and share their data.

Clarifying how existing national laws apply in cyberspace and developing new balanced frameworks to address abuses, will enable the digital economy to protect human rights and will determine the shape of the emerging digital economy. To preserve the open, cross-border nature of the internet, policy coherence and legal interoperability between multiple regimes must be established. This requires communication, coordination and, ultimately, cooperation among all stakeholders.

Yet, sound policy-making must be based on evidence and reliable data. Policy coherence on a transnational basis can only be achieved through a shared understanding of the issues at stake and awareness of the various initiatives. The availability of this comprehensive overview and analysis of trends and initiatives will translate the highly complex and often technical nature of substantive issues for decision makers. This Report represents the first step of an ongoing effort by the Secretariat of the Internet & Jurisdiction Policy Network to make this essential information accessible to all stakeholders, to help them to collectively address some of the most pressing global challenges of our times.

We are delighted that this full edition of the Internet & Jurisdiction Global Status Report will be launched on the occasion of the 14th Internet Governance Forum in Berlin, Germany. We would like to express our gratitude to the pioneers of this new global effort to foster policy coherence through capacity building and evidence-based policy innovation: the stakeholders in the Internet & Jurisdiction Policy Network, the author, Professor Dan Svantesson, as well as Germany, Denmark, Estonia and the European Commission, who are making this essential effort possible.

DR. MARIA FLACHSBARTH
Parliamentary State Secretary to the Federal Minister for Economic Cooperation and Development, Germany

The World Wide Web, the internet as most people know it, is just 30 years old. Within this short amount of time, the distinction between the online and offline world has become meaningless. We are online every day. We use the internet to receive news. We communicate with family, friends and co-workers. Our homes and appliances are connected through the Internet of Things. We order business services and interact with local and national authorities. Our mobile phones and laptops make for easy internet access at home or on the go.

The internet increased global connectivity, advanced our societies and economies, and still offers tremendous opportunities. However, we must not forget that almost half the world's population has no access to the internet. Particularly, women are facing inequalities with regard to access to the internet and participation in the IT sector. The internet's potential still needs to be unlocked in remote areas and less developed countries. This is a task of utmost importance, and we need to keep it in mind when talking about the internet's future and evolution. Also, not all countries and stakeholders have been able to contribute equally to discussions about internet jurisdiction and regulation.

The internet established some new challenges, too. Free speech needs to be protected online and we have to find ways to deal with hate speech, manipulation and misinformation. Data security and privacy rights are of highest importance and we require a defence against mounting cyber threats. Eventually, we need to have a secure but open and reliable internet that benefits all, people and businesses around the world.

Germany advocates for net neutrality, free speech and access for all. The Federal Ministry of Economic Cooperation and Development cooperates closely with developing countries in digitalisation processes and promotes the inclusion of developing countries in all relevant discussions. That is why we supported this very first Internet & Jurisdiction Global Status Report.

We wish for the progressing debate on jurisdictional challenges to the open internet to be inclusive, to involve all stakeholders and to be open for all regions of the world.

CASPER KLYNGE
Danish Tech-ambassador
Ministry of Foreign Affairs of Denmark

Digitalisation and technology are defining parameters for how our societies evolve in the 21st century. On the one hand, technology has the potential to lift people out of poverty, improve healthcare and other key sectors of society and drive economic growth. On the other hand, technology could exacerbate inequalities, undermine fundamental rights and erode public trust in democratic institutions. To reap the benefits and minimise the risks of technological development, a balanced approach is necessary. This requires the right policy framework. We therefore need to identify the challenges technology presents to governance at both the national and international level. Cross-border technologies, such as the internet and platform economy, bring a range of such challenges.

Denmark therefore welcomes the Internet & Jurisdiction Policy Network's effort to map the major trends of the digital society. The Internet & Juristiction Global Status Report is a timely contribution towards a better understanding of the digital age, which is an important step in providing us with a solid base for constructive international dialogue and cooperation. Approximately two years ago, the Danish government decided to elevate technology and digitisation to a strategic foreign policy priority – through the TechPlomacy-initiative – and to appoint Denmark's, and in fact the world's first, Ambassador for Technology and Digitization ('Tech Ambassador') and to create a dedicated representation to technology. The initiative is a response to the increasing importance that technology, digitalisation and the industry has on individuals, societies and international relations alike – and the necessity of boosting the dialogue between the tech industry, governments and multilateral organisations. We are working towards a stronger multistakeholder cooperation to ring-fence core values and institutions and to promote a human-centric approach to technological development. In short, a balanced approach where public and private actors take responsibility. In recognition of the urgent need for common norms and the perseverance of a rules-based international order in the digital era. To get regulation right and to safeguard democracy, human rights and the rule of law.

Digitalisation is international and cross-border in nature, creating a number of new legal and other challenges to our societies and the rule of law in the digital age – an age that for the very same reason requires more, not less, international cooperation.

HELI TIIRMAA-KLAAR
Ambassador at Large for Cyber Diplomacy,
Ministry of Foreign Affairs of Estonia

In 2018, the world reached an important milestone as more than 50% of its population had gained access to the internet. As demonstrated in the Internet & Jurisdiction Global Status Report, the internet has already revolutionized how people, businesses and governments interact. The multistakeholder governance model of the internet has provided a platform for enormous economic development and political progress globally. In order to continue this progress, it is critical that the accountable multistakeholder model of the internet will be maintained, even if the growing interdependence on cyberspace seems to be creating unprecedented challenges. Although open, free and accessible cyberspace is, for many states, part of their democratic identity, for some, internet governance may be seen as yet another tool for executing state control. Estonia has always supported the open and interoperable internet. Non-discriminatory access to and accessibility of the internet are fundamentally important for enabling and promoting the right to freedom of expression, assembly and association. Access to independent media sources, social media platforms and a free Internet has become an integral part of good governance and democratic society. While it should be clear that the existing international law applies to cyberspace, there is a need to further develop and implement norms of responsible state behaviour in this dynamic field. This evidently requires communication, coordination and cooperation among all stakeholders.

The Internet & Jurisdiction Global Status Report focuses on the overarching and topical trends, as well as legal and technical approaches, and creates links between different global and regional initiatives. One of the incentives for this Report was to enable better access to relevant information, particularly the existing laws and their application. However, there still is a clear need for a meaningful coordination between multiple actors in the field and the existing initiatives. The Report provides a comprehensive overview and documentation of the past, current and emerging trends. It also contributes to the global discussion on possible solutions for the major cross-border legal policy challenges. As a co-sponsor of the Report, Estonia is hoping to create bridges between the different initiatives and jurisdictions. We are certain that this Report will contribute to better coordination among different stakeholders for developing and protecting an interoperable and secure internet for the global multistakeholder community.

PEARSE O'DONOHUE
Director for Future Networks
DG CONNECT, European Commission

The internet has already been in our lives for decades. It is now a critical means for transformation of our economies and societies, and its importance will continue to grow. So, it is our responsibility to ensure that the internet remains a human-centric, safe and trusted environment.

The EU's Digital Single Market strategy has achieved a lot in this respect. It has given European citizens, businesses, and public administrations new working and living opportunities in a safe and inclusive way, providing fair access to digital goods, content and services. Digital trust has been enhanced through the application of the General Data Protection Regulation, and the improvement of the EU's resilience to cyber-incidents through a new Cybersecurity framework. With the DSM, the EU has provided concrete and tangible benefits to European citizens, but it has also taken a leading role in setting reference policy standards for the digital era.

The internet is, of course, a global phenomenon, and it is our ambition to drive the global policy debate on the internet with our partners and all stakeholders who share our values, as part of the multistakeholder approach to internet governance. This debate, which has traditionally focused on core internet infrastructures, needs to be broadened to cover issues such as the governance of Artificial Intelligence, the free flow of data and trust on the internet. Jurisdictional issues such as liability in the case of services offered over the internet, the choice of law in event of dispute or the recognition of national laws and their enforcement, are also important. In addressing these issues, we must not allow accusations of protectionism to deflect us from maintaining a high level of protection of the individual. The Internet & Jurisdiction Global Status Report 2019 offers a useful overview of the overarching trends affecting the cross-border nature of the internet. We welcome the effort of tracking legislative initiatives globally, soft law measures and best practices on the internet. This mapping exercise will certainly enrich the internet governance debate and stimulate the multistakeholder community in finding solutions to online jurisdictional problems. This is an important discussion to have if we want to maintain one global internet.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This Report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network.

The production of this Report was enabled by financial support provided by the German Corporation for International Cooperation (GIZ) on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ), the Ministry of Foreign Affairs of Denmark, the Ministry of Foreign Affairs of Estonia and institutional support was provided by the European Commission, Directorate-General for Communications Networks, Content and Technology (DG CONNECT).

AUTHORSHIP TEAM:

AUTHOR:
Professor Dr. Dan Jerker B. Svantesson
Bond University
Gold Coast
Australia

RESEARCH AND
INTERVIEW ASSISTANCE:
Rebecca Azzopardi
Ph.D. Candidate
Bond University
Gold Coast
Australia

PROJECT COORDINATION:

Martin Hullin
Head of Operations and Partnership Manager
Secretariat of the Internet & Jurisdiction Policy Network

PROJECT TEAM:

Bertrand de la Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

Xavier Guyot de Camy
Policy Manager
Secretariat of the Internet & Jurisdiction Policy Network

Ajith Francis
Policy Officer
Secretariat of the Internet & Jurisdiction Policy Network

PRODUCTION:

Secretariat of the Internet & Jurisdiction Policy Network, Paris, France

EDITING:

Emma Dann, Bond University, Gold Coast, Australia

DESIGN AND LAYOUT:

Formas do Possível - Creative Studio, Lisbon, Portugal

The Secretariat greatly appreciates the time and contribution of all participating survey respondents and interviewees. Without their valuable insights, this report could not have been produced.

Waiswa Abudu Sallam
Head Legal Affairs
Communications Commission
Uganda

Benedict Addis
Chair
Registrar of Last Resort (RoLR)
UK

Fiona Alexander
Associate Administrator for International Affairs
Department of Commerce
National Telecommunications and Information Administration (NTIA)
USA

Chinmayi Arun
Assistant Professor of Law
National Law University Delhi
India

Karen Audcent
Senior Counsel
Department of Justice
Canada

Greg Aaron
Vice-President
iThreat
USA

Halefom Abraha
Research Officer
Information Policy and Governance
University of Malta
Malta

Bakhtiyor Avezdjanov
Program Officer
Columbia University, Global Freedom of Expression
USA

Adriele Ayres Britto
Senior Counsel
Ayres Britto Consultoria Jurídica e Advocacia
Brazil

Kerry Ann Barrett
Cybersecurity Policy Specialist
Organization of American States (OAS)
USA

Elizabeth Behsudi
Former General Counsel
Public Interest Registry (PIR)
USA

Tijani Ben Jemaa
Executive Director
Fédération Méditerranéenne des Associations d'Internet (FMAI)
Tunisia

Eduardo Bertoni
Director
National Access to Public Information Agency
Argentina

Theo Bertram
Public Policy Manager
Google
USA

Aparajita Bhatt
Assistant Professor
National Law University Delhi
India

Ellen Blackler
Vice President
Global Public Policy
The Walt Disney Company
USA

Marko Bošnjak
Judge
European Court of Human Rights (ECHR)
France

Maarten Botterman
Board Director
The Internet Corporation for Assigned Names and Numbers (ICANN)
Netherlands

Andrew Bridges
Partner
Fenwick & West LLP
USA

Lisl Brunner
Director
Global Public Policy
AT&T
USA

Andre Caissy
Senior Policy Analyst
Canada, Department of Canadian Heritage
Canada

Brent Carey
Domain Name Commissioner
Domain Name Commission for .nz
New Zealand

Jordan Carter
Chief Executive
InternetNZ
New Zealand

Mark Carvell
International Online Policy Senior Adviser
Department for Digital Culture, Media and Sport (DCMS)
UK

Adriana Castro Pinzón
Deputy Director
Business Law Department
Universidad Externado de Colombia
Colombia

Eileen Berenice Cejas
Communications Director
Digital Grassroots
Argentina

Angelica Chinchilla-Medina
Director
Ministry of Science, Technology and Telecommunications
Costa Rica

Vivian Choy
Crime and Intelligence Analyst
Canada, Calgary Police Service
Canada

Jose Clastornik
Executive Director
AGESIC - National eGovernment and Information Society Agency
Office of the President of Uruguay

Alexander Corbeil
Senior Research Analyst
Canada, Public Safety
Canada

Alexander Corbeil
Research Advisor
Canada, Public Safety
Canada

Jennifer Daskal
Associate Professor
American University
Washington College of Law
USA

Bertrand De la Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction
Policy Network
France

Sissi Maribel De La Peña
Director of e-business and international organizations
ALAI - Asociación Latinoamericana de Internet
Mexico

Jacques De Werra
Professor
University of Geneva
Switzerland

Agustina Del Campo
Director
Center for Studies on Freedom of Expression and Access to Information (CELE)
Argentina

Steven Delbianco
President
NetChoice
USA

Fernanda Domingos
Federal Prosecutor
Federal Prosecution Service
Brazil

Valensiya Dresvyannikova
Policy and Research Officer
International Federation of Library Associations and Institutions (IFLA)
UK

Salomé Eggler
Advisor
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Germany

Shruttima Ehersa
Associate
Inttl Advocare
India

Brendan Eiffe
Head of Mutual Legal Assistance
Division Department of Justice and Equality
Ireland

Miriam Estrin
Policy Manager
Google
UK

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network
France

Benedicto Fonseca Filho
Ambassador
Ministry of Foreign Affairs
Brazil

Nils Finder
Referent, Governance & Markets, Government Affairs
Siemens AG
Germany

Julia Fossi
Expert Advisor
eSafety Commissioner
Australia

Gary Fowlie
Advisor
Geeks Without Frontiers
USA

Jothan Frakes
Executive Director
The Domain Name Association
USA

Eric Freyssinet
Chief Digital Strategy Officer
Gendarmerie nationale
France

Giancarlo Frosio
Senior Lecturer
University of Strasbourg
CEIPI
France

Lise Fuhr
Director General
European Telecommunications Network Operators' Association (ETNO)
Belgium

Chawki Gaddes
Président
Instance Nationale de Protection des Données Personnelles (INPDP)
Tunisia

Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa
Canada

Jan Gerlach
Senior Public Policy Manager
Wikimedia Foundation
USA

Lorna Gillies
Senior Lecturer
Strathclyde University
UK

Grace Githaiga
Co-convenor
Kenya ICT Action Network (KICTANet)
Kenya

Hartmut Glaser
Executive Secretary
Brazilian Internet Steering Committee/CGI.br
Brazil

Tonei Glavinic
Director of Operations
Dangerous Speech Project
Spain

Joaquín Gonzalez-Casanova
Director General for International Affairs
Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales
Mexico

Luca Grandi
Legal Counsel
Ferrero
Luxembourg

Robyn Greene
Privacy Policy Manager
Facebook
USA

Nicole Gregory
Head Data and Online Harms,
Foreign & Commonwealth Office
UK

Robert Guerra
CEO
Privaterra
Canada

Devesh Gupta
Manager
Reliance Industries Limited (RIL)
India

Hiroki Habuka
Deputy Director, Digital Economy Division
Ministry of Economy, Trade and Industry (METI)
Japan

Statton Hammock
Vice-President
MarkMonitor
USA

Sara Harrington
Vice President Legal
Chen Zuckerberg Foundation
USA

Byron Holland
President and CEO
Canadian Internet Registration Authority (CIRA)
Canada

Daniel Holznagel
Legal Officer
Federal Ministry of Justice and Consumer Protection
Germany

Martin Husovec
Assistant Professor
Tilburg University
Netherlands

Erick Iriarte
Senior Partner
Iriarte & Associates
Peru

Manal Ismail
Executive Director
International Technical Coordination
National Telecom Regulatory Authority (NTRA)
Egypt

Pavlina Ittelson
Program Manager
DiploFoundation
Switzerland

Sunali Jayasuriya
Legal Officer
Information and Communication Technology (ICT) Agency
Sri Lanka

Tarek Kamel
Senior Advisor
The Internet Corporation for Assigned Names and Numbers (ICANN)
Egypt

Seb Kay
Policy Adviser
Foreign & Commonwealth Office
UK

Daniel Keck
Adviser
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Germany

Daphne Keller
Director of Intermediary Liability
Stanford Law School Center for Internet and Society
USA

Gail Kent
Global Public Policy Lead on Law Enforcement and Surveillance
Facebook
USA

Tshoganetso Kepaletswe
Chief Technology Officer
Communications Regulatory Authority
Botswana

Matthias Kettemann
Co-Head
Research Focus Internet & Society
University of Frankfurt/Main
Germany

Gayatri Khandhadai
Asia Policy Regional Coordinator
Association for Progressive Communications (APC)
India

Jan Kleijssen
Director of Information Society and Action against Crime
Council of Europe
France

Wolfgang Kleinwächter
Professor
Global Commission on the Stability in Cyberspace (GCSC)
Germany

Casper Klynge
Tech Ambassador
Ministry of Foreign Affairs
Denmark

Monika Kopcheva
Political Administrator
Council of the EU
Brussels

Dominique Lazanski
Director
Public Policy and International Relations
GSMA
UK

Emmanuelle Legrand
Legal and Policy Officer
European Commission (EC)
Belgium

May-Ann Lim
Executive Director
Asia Cloud Computing Association and Managing Director, TRPC Pte Ltd
Singapore

Rebecca Mackinnon
Director
Ranking Digital Rights
New America
USA

Dinesh Mandagere
Managing Consultant
Wipro
India

Giacomo Mazzone
Head of Institutional Relations
European Broadcasting Union (EBU)
Switzerland

Corynne McSherry
Legal Director
Electronic Frontier Foundation (EFF)
USA

Christine Mackenzie
President
International Federation of Library Associations and Institutions (IFLA)
Netherlands

Patricia Miranda
Senior Counsel
World Bank
USA

Roudabeh Moghaddam
Executive Secretary to the Steering Committee
Child Dignity Alliance
UK

Doris Möller
Counsel
Association of German Chambers of Industry and Commerce
Germany

Francesca Musiani
Associate Research Professor (eq.)
Centre Nationale de la Recherche Scientifique (CNRS)
France

Vivek Narayanadas
Data Protection Officer
Shopify
Canada

Victoria Nash
Senior Policy Fellow
University of Oxford
UK

Gonzalo Navarro
Chief Executive Officer
Latin American Internet Association (ALAI)
Chile

Paul Nemitz
Principal Adviser
European Commission (EC)
Belgium

Michele Neylon
Chief Executive Officer
Blacknight Internet Solutions Ltd
Ireland

Gregory Nojeim
Director
Freedom, Security & Technology Project
Center for Democracy & Technology (CDT)
USA

Elliot Noss
Chief Executive Officer
Tucows
Canada

Michael Oghia
Advocacy & Engagement Manager
Global Forum for Media Development
Serbia

Seun Ojedeji
Chief Network Engineer
Federal University Oye-Ekiti
Nigeria

Phol Edward Paucar Aguirre
Universidad del Pacífico
Peru

Elena Perotti
Executive Director Public Affairs and Media Policy
World Association of Newspapers and News Publishers (WAN-IFRA)
France

Christian Perrone
Google Public Policy Fellow
Institute for Technology and Society of Rio de Janeiro (ITS Rio)
Brazil

Nick Pickles
Senior Public Policy Strategist
Twitter
USA

Jason Pielemeier
Policy Director
Global Network Initiative (GNI)
USA

Marc Porret
Legal and Criminal Justice Coordinator
United Nations Counter-Terrorism Committee Executive Directorate (UNCTED)
USA

Frederic Potier
National Delegate
Délégation Interministérielle à la Lutte Contre le Racisme l'Antisémitisme et la Haine anti-LGBT (DILCRAH)
France

Rosanna Rafel-Rix
Digital Media Manager
Community Security Trust
UK

Rod Rasmussen
Principal
R2 Cyber
USA

Chris Riley
Director
Public Policy
Mozilla
USA

Beatriz Rodríguez
Adviser
Unidad Reguladora y de Control de Datos Personales (URCDP)
Uruguay

Jorge Rodríguez-Zapata
Justice
Supreme Court
Spain

Elettra Ronchi
Head of Unit
Organization for Economic Co-operation and Development (OECD)
France

Kostas Rossoglou
Head of EU Public Policy
Yelp
Belgium

Alexandre Roure
Senior Manager
Public Policy, Computer & Communication Industry Associations (CCIA)
USA

Stefan Saatmann
Global Cybersecurity Policy Coordinator
Siemens AG
Germany

Nicolás Schubert
Digital Economy Coordinator
General Directorate of International Economic Affairs
Ministry of Foreign Affairs
Chile

Lori Schulman
Senior Director
Internet Policy
International Trademark Association
USA

Jörg Schweiger
Chief Executive Officer
DENIC eG
Germany

Amy Shepherd
Legal and Policy Officer
Open Rights Group
UK

Toussi Simone
Researcher
South Lights 2030
Cameroun

Tim Smith
General Manager
Canadian International Pharmacy Association
Canada

Alissa Starzak
Head of Public Policy
Cloudflare
USA

Christoph Steck
Director
Public Policy
Telefonica
Spain

Blair Stewart
Assistant Commissioner
Office of the Privacy Commissioner
New Zealand

Peter Swire
Professor
Georgia Tech Scheller College of Business
USA

Ian Toon
Digital Examiner
London Metropolitan Police
UK

Stanislaw Tosza
Assistant Professor
Utrecht University
Netherlands

Takahiko Toyama
Director for Information Policy Planning
Ministry of Economy, Trade and Industry (METI)
Japan

Lee Tuthill
Counsellor
World Trade Organisation (WTO)
Switzerland

Kimmo Ulkuniemi
Chief Superintendent
National Police Board
Finland

Peter Van Roste
General Manager
CENTR
Belgium

Mark Villiger
Retired Judge
Formerly Section President
European Court of Human Rights (ECtHR)
France

Ian Walden
Professor of Information and Communications Law
Queen Mary University of London
UK

Shota Watanabe
Researcher
Nomura Research Institute, Ltd.
Japan

Rolf H. Weber
Professor of International Business Law
University of Zurich
Switzerland

Paul Wilson
Director General
Asia-Pacific Network Information Center (APNIC)
Australia

Shinichi Yokohama
Chief Information Security Officer
Nippon Telegraph & Telephone (NTT)
Japan

Nicolo Zingales
Lecturer
Sussex University
UK

EXECUTIVE SUMMARY

Introduction

The Internet & Jurisdiction Global Status Report 2019 is the world's first comprehensive mapping of internet jurisdiction related policy trends, actors and initiatives. It is based on an unprecedented large-scale data contribution from 150 key stakeholders from the Internet & Jurisdiction Policy Network from: states, internet companies, technical operators, civil society, academia and international organizations.

The surveyed stakeholders send a very **strong message of concern**:

- 95% see cross-border legal challenges on the internet becoming increasingly acute in the next three years[1];
- Only 15% believe we already have the right institutions to address these challenges[2]; and
- 79% consider that there is insufficient international coordination[3].

50 years after the creation of the internet, the Report presents strong evidence of a **dangerous trend**: the worldwide multiplication of public and private policy initiatives in an uncoordinated manner will have detrimental consequences. Even when they legitimately aim to address key transnational policy issues, adoption of quick-fix measures under the pressure of urgency often leads to a legal arms race and additional conflicts. Making sure that the fundamental attributes of the internet are preserved requires active steps in the form of **innovative coordination and cooperation efforts**.

Issues and initiatives proliferate

Stakeholders express their difficulty to access comprehensive information on numerous and complex policy challenges, as well as to keep track of the proliferating initiatives trying to address them. Yet, consolidated and accessible data is a prerequisite for evidence-based decision-making and policy coherence.

Accordingly, the Report extensively documents the increasing number of **topics of concern** that demand attention, be they related to expression, security or the digital economy. Jurisdictional challenges arise in all instances of online regulation, such as the regulation of:

- Violent extremism, hate, data privacy breaches, and other forms of abuse that may become so prevalent that the online environment becomes 'uninhabitable', while an actual or perceived high degree of misinformation causes a trust crisis;
- Cybercrime and cyber attacks that may durably undermine trust in the online environment and threaten its infrastructure; and
- Commercial activities in relation to which complexity increases the cost of compliance and may create barriers to entry for small and medium enterprises, limiting competition, innovation, and market access across borders.

AT A GLANCE...

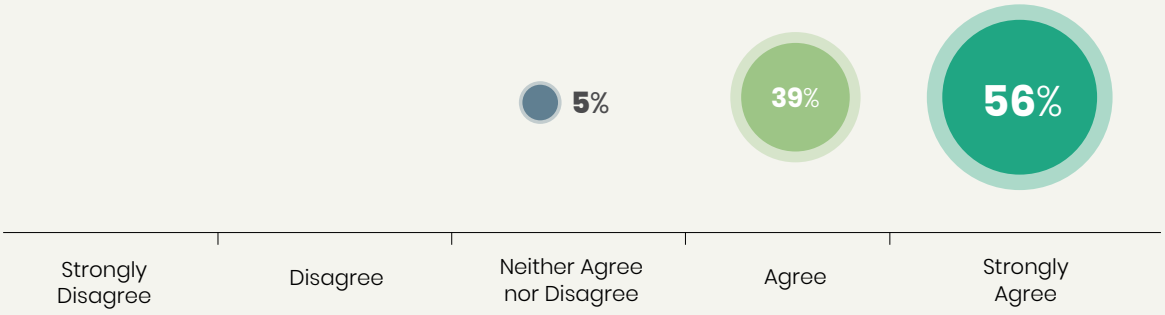
- Cross-border legal challenges on the internet are increasingly acute.
- Normative plurality in cyberspace is rising.
- The risk of a harmful legal arms race is very high.
- Important human rights are at stake.
- Important economical and societal interests are at stake.
- Cyberspace risks being fragmented along national borders.
- Online abuses risk not being addressed efficiently in the absence of cooperation.
- Developing countries and SMEs are facing significant regulatory barriers.
- The regulatory agenda is set by a small number of dominant states and other actors.
- The governance ecosystem is characterized by competing agendas and values.
- The regulatory complexity is increasing, leading to legal uncertainty.
- Central legal concepts are outdated and prevent progress.
- Private actors are increasingly performing quasi-public regulatory and judicial roles.
- Stakeholders call for appropriate institutions, frameworks and policy standards.
- Stakeholders call for greater international coordination.
- Stakeholders call for inclusiveness and capacity building.
- Stakeholders stress the value of multistakeholderism.

---

1. Infographic 4, page 28
2. Infographic 6, page 33
3. Infographic 8, page 35

INFOGRAPHIC 1

Will cross-border legal challenges on the internet become increasingly acute in the next three years?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

The Report also documents the increasingly diverse **legal or technical approaches** adopted by governments and private actors to address these issues including:

- Extraterritorial assertion of jurisdiction;
- Private terms of service and community guidelines;
- Mandatory data localization; and
- Geo-blocking.

The Report points to several key challenges when addressing cross-border legal issues, that **put at stake fundamental attributes of the cross-border internet**, such as:

- The lack of common agreement on substantive values between actors, or shared understanding of key legal concepts and vernacular;
- The risk of a "race to the bottom" if extraterritoriality is not implemented with caution;
- distrust generated amongst internet users who cannot know what laws apply to their online activities;
- Voluntary or involuntary fragmentation, both in a technical and a regulatory sense, may develop to such a degree that it becomes impossible to speak of the internet as a global network; and
- A failure to strike an appropriate balance in the obligations imposed on internet intermediaries may result in an extensive loss of online freedom of expression and the availability of services to the extent that the very nature of the current cross-border internet is affected.

Legal uncertainty dominates

Much of what has been done to date sought to solve global problems through a national lens. However, the constant flux of digital innovation and the transnational nature of the internet makes it increasingly challenging to address online abuses with traditional national legal tools.

Moreover, as transnational interactions become the new normal, people and entities are often unable to determine their "contextual legal environment", i.e.: all the states' laws and other norms that apply to their activity online at a given moment.

Due to extraterritorial assertions of jurisdiction, in some regions, individuals, organizations and even states are concerned that they are subjected to online rules developed without them in a country far away.

A dangerous spiral

A legal arms race of uncoordinated, reactive, and quick-fix public and private policy initiatives, prone to be incompatible, creates a dangerous spiral, detrimental on numerous levels because it:

- Creates competing assertions of jurisdiction where compliance with one state's law unavoidably results in a direct violation of other states' laws;
- Actually prevents actors from efficiently addressing abuses online;
- Hampers digital innovation and growth of the internet economy, especially in developing countries and for SMEs; and
- Favors the rule of the strongest.

This could make cross-border online spaces and activities potentially impossible in the future.

Coordination is a must

The stakes are high: the internet deeply impacts all societies and economies and new regulatory frontiers are constantly emerging, ranging from cryptocurrencies to artificial intelligence. Much like the natural environment is facing a climate change, the online legal environment is now also undergoing a systemic transformation.

There is much that needs to change in order to overcome the cross-border legal challenges. The surveyed stakeholders specifically pointed to the need for:

- More coordination to ensure policy coherence;
- More legal interoperability, through both substantive and procedural standards that are jointly developed;
- Inclusiveness and capacity building, including addressing practical issues such as lack of access to relevant information due to language and cultural barriers, as well as information overload;
- Greater clarity, and a common understanding, of relevant legal concepts;
- Considering the respective roles of the private and the public sector, including a clear need for re-examining and more clearly defining the roles of intermediaries;
- Transparency and accountability;
- Pursuing solutions on an issue-by-issue basis, or as clusters of issues;
- Continued, or even expanded, adherence to a multistakeholder approach; and
- A recognition that no state, company or organization can address these issues alone, and that actors in the ecosystem simply cannot afford not to collaborate.

Shaping the future of the digital society

Stakeholders of the Internet & Jurisdiction Policy Network stressed that, in the end, not addressing jurisdictional challenges would come at a high cost: the question now is not whether to regulate but how, and by whom. As pointed out by one surveyed expert, the internet is neither the problem, nor the cause of the problem. Indeed, the internet risks becoming the victim of our lack of appropriate governance mechanisms.

The task that lies before us all demands governance innovation: it involves developing the standards for legal interoperability and policy coordination, so that we are equipped with methods and tools that are as transnational, distributed, scalable and resilient as the internet itself. What is at stake is nothing less than the future of the digital society that we collectively want – for us and for future generations.

Method

It is daunting to embark on a mapping and analysis exercise aimed at facilitating a comprehensive understanding of a highly complex and dynamic ecosystem – one comprised of multiple actors, initiatives and trends across the policy silos of the digital economy, human rights and security. Such an undertaking presents several challenges. Most obvious is the difficulty in facilitating a sufficiently deep understanding of the complex issues associated with the coexistence of heterogeneous laws on the cross-border internet – one of the greatest policy challenges of the 21st century.

Furthermore, there are challenges associated with seeking to fully understand, and represent fairly, the diverse views and multifaceted interests involved. Another considerable challenge is that of the so-called 'unknown unknowns'; with any research task involving great sectoral and geographical diversity comes a risk of missing something important without even realizing that it is missing.

An awareness of such challenges shaped the method of this report, and led to the adoption of a flexible, qualitative research design that enables an in-depth exploration of the research questions. To overcome the challenges cited above, this writing project has adopted a multifaceted research method incorporating an unprecedented and innovative large-scale collaborative contribution and review process. This process leveraged the combined expertise of the key stakeholders engaged in the Internet & Jurisdiction Policy Network through semi-structured interviews, peer review feedback and data collection procedures, combined with detailed and extensive desk research.

The desk-research

Desk research adopted conventional legal research methods and consisted primarily of a comprehensive study and analysis of relevant case law, legislation and other regulatory initiatives, as well as the literature – including books, journal articles, published conference papers and industry publications. This was supplemented with a detailed study of a variety of valuable reports and other materials from a range of bodies over recent years.

The desk research benefited greatly from the Internet & Jurisdiction Policy Network's wide-ranging collection of relevant developments available in the I&J Retrospect Database.[4] The Retrospect Database is the flagship, open-access publication of the Internet & Jurisdiction Policy Network, documenting policy developments, judicial decisions, international agreements and other cases that reflect jurisdictional tensions on the cross-border internet. This important collection provided up-to-date insights into current major trends, attitudes, developments and initiatives.

The materials contained in the Retrospect Database also provided important insights into current legal and technical approaches to solutions, as well as in relation to what this Report defines as overarching 'meta-trends'.

The first stakeholder survey

The first method for gaining stakeholder input consisted of an online survey made up of 17 questions on a variety of topics relevant for the research questions. In considering how best to gather survey data to inform the research questions, great care was taken to design questions that may be answered by any of the relevant stakeholders. This ensured that all survey participants were exposed to the same set of questions.

The Internet & Jurisdiction Policy Network Secretariat identified survey participants representing all of its stakeholder groups – i.e., academia, civil society, governments, international organizations, internet platforms and the technical community – and participants were specifically selected to guarantee geographical diversity. To that end, specific geographic regions were targeted to capture as much variation as is possible. Furthermore, the selection of the survey participants was purposive, in that they were specifically targeted based on their considerable expertise and knowledge. In total, input was received from 100 survey participants during a period from Autumn 2018 to Spring 2019. Participants provided their views in their personal capacities, rather than as representatives of any specific organization. Furthermore, input gained from the surveys has only been used without attribution.

The expert input gained from the survey was invaluable. Apart from bringing attention to major topical trends, approaches to solutions, overarching meta-trends and generally held concerns in the ecosystem, the survey results helped provide both context and a more nuanced understanding of the operating environments facing civil society, governments, international organizations, internet platforms and the technical community.

Survey results are used throughout the Report to show, in figures, the concerns and attitudes of the Internet & Jurisdiction Policy Network's stakeholder ecosystem. In addition, the comments from surveyed experts are used to highlight particularly important arguments, observations and concerns.

---

4. Internet & Jurisdiction Policy Network. *I&J Retrospect Database.* Retrieved from https://www.internetjurisdiction.net/publications/retrospect.

Stakeholder interviews

Semi-structured interviews were organized across a broad range of stakeholders in order to complement the insights gained from the survey responses and desk research. As with the surveys, the Internet & Jurisdiction Policy Network Secretariat took care to ensure inclusiveness and diversity, with the selected interviewed experts representing academia, civil society, governments, international organizations, internet platforms and the technical community, with geographical diversity. These stakeholders were identified both from within and outside the Internet & Jurisdiction Policy Network.

Each interview lasted over 30 minutes, on average. The interviews were conducted in confidence and as such, were not recorded. Detailed notes were collated, however, and observations were recorded in a structured manner, facilitating cross-referencing and detailed analysis.

The semi-structured interviews allowed for considerable flexibility and catered for supplementary questions based on discussions with the interviewee. This – combined with the confidentiality guarantee – provided an environment in which interviewed experts could highlight matters important to them within the topics discussed. In many cases, the interviewees could also provide perspectives, insights and information that might otherwise have been unattainable by researchers. In this way, part of the purpose of the interviews was to reduce regional and topical gaps in the desk research. In total, 63 interviews were carried out from Autumn 2018 to Spring 2019. The interviewed experts provided their views in their personal capacities rather than as representatives of any specific organization. Furthermore, input gained from the interviews has only been used without attribution.

Like the comments made by surveyed experts, the interviewed experts' comments were vital and are used throughout the Report to highlight particularly important arguments, observations and concerns.

Stakeholder feedback

Apart from the surveys and interviews, stakeholder input was sought by sharing an advanced version of the Report with contributors prior to the 3rd *Global Conference of the Internet & Jurisdiction Policy Network* held June 3-5, 2019 at which almost 300 key stakeholders from over 50 countries gathered in Berlin. A shorter – Key Findings – version of this Report was launched at the 3rd *Global Conference of the Internet & Jurisdiction Policy Network*.

The input gained from this review was tremendously valuable and has helped ensure the quality of this Report, particularly by minimizing regional and topical gaps.

> "The expert input gained from the survey was invaluable. Apart from bringing attention to major topical trends, approaches to solutions, overarching meta-trends and generally held concerns in the ecosystem, the survey results helped provide both context and a more nuanced understanding of the operating environments facing civil society, governments, international organizations, internet platforms and the technical community."

The second stakeholder survey

A second stakeholder survey was held during the third quarter of 2019. This survey took the form of an open call inviting interested parties to provide general input for the Report. In addition, the survey sought specific input to complement the lists of current initiatives and developments collected via the desk research, first survey and the interviews.

The second survey generated valuable input from over 50 contributors. This input further helped ensure the quality of this Report, particularly by minimizing regional and topical gaps.

Limitations of the study

A research study of this nature carries certain limitations. First, the scope of the Report is delineated by reference to the Internet & Jurisdiction Policy Network's mandate. Thus, this is not a global status report generally about the Internet; rather it is specifically focused on cross-border legal issues in relation to the internet. Second, despite the steps outlined above, the inevitable risk of gaps must be acknowledged. The statistical relevance of exploratory research relying, in part, on a limited number of survey participants and interviewed experts should not be overstated. In addition, most forms of desk research may be accused of involving biases that are difficult to eliminate in full.

In light of the above, this Report represents a best-effort attempt at painting a broad-brushed, yet comprehensive, overview and documentation of past, current and emerging trends, relevant actors, and proposed solutions to the major cross-border legal policy challenges facing our connected society as of 1 July 2019. As such, it is a timely snapshot of the policy environment and creates a first baseline against which future studies may be undertaken.

01

WHY A GLOBAL STATUS REPORT, AND WHAT IS AT STAKE?

EXPRESSION

SECURITY

ECONOMY

1.1

Responding to the call from the Internet & Jurisdiction Policy Network

The Internet & Jurisdiction Global Status Report 2019 is the first of its kind. It is produced in response to the urgent call of over 280 senior-level stakeholders from 50 countries at the 2nd and 3rd Global Conference of the Internet & Jurisdiction Policy Network in 2018 and 2019.

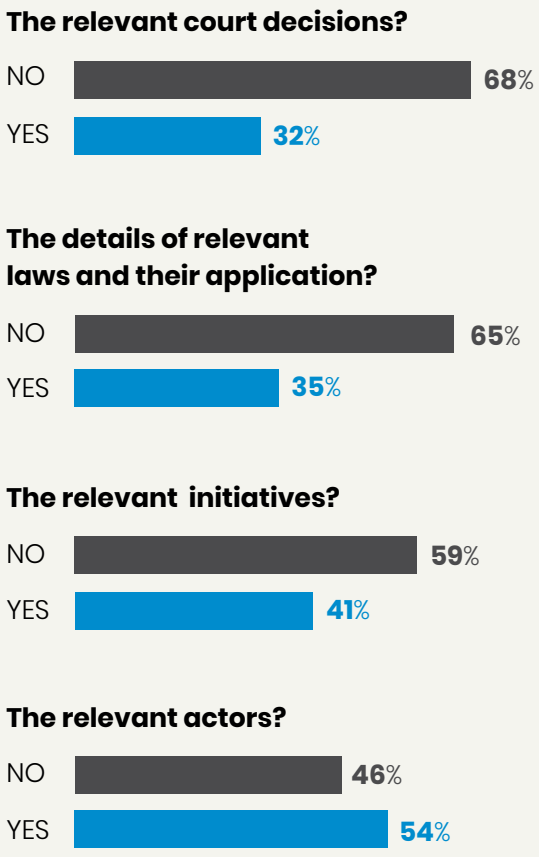
The primary aim of the Global Status Report is to provide a snapshot of the current landscape and to reflect the current thinking, concerns, trends and proposals of the Internet & Jurisdiction Policy Network's diverse stakeholders. Thus, the aim is to provide both an objective assessment of what this ecosystem of stakeholders faces today, and to anticipate relevant developments by, for example, highlighting overarching trends that will impact developments for the foreseeable future.

A secondary aim is for the Global Status Report to be a useful resource for capacity building, and for creating a greater understanding of the complicated issues involved – issues that stand to profoundly affect the entire ecosystem. To a degree, the Report may also provide a much-needed baseline for future studies of legal and regulatory trends at a global level, and it serves as a point of departure for the Internet & Jurisdiction Policy Network's forthcoming Regional Reports.

Surveyed experts were asked whether they currently have easy access to enough information about relevant actors, initiatives, laws and court decisions. While the survey highlighted some regional and sectoral differences, it also identified a clear need for better access to relevant information.

INFOGRAPHIC 2

On the topic of cross-border legal challenges on the internet, do you currently have easy access to enough information about:



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

As these results make clear, there is considerably greater access to sufficient information about relevant actors[5] and initiatives, than to information about the details of relevant laws and their application, or to relevant court decisions. Stakeholders from non-OECD countries indicated a considerably lower degree of easy access to information about the relevant actors and initiatives, which suggests a need for capacity building and outreach to facilitate ongoing and future conversations.

When asked whether there is easy access to enough information about the details of relevant laws and their application, the answer was a resounding 'no' across regions and stakeholder groups, apart from academia. No less than 50% of respondents from academia indicated that they have easy access to such information, implying that the problem is not an absence of information, but rather relates to the accessibility of such information. This can be partly explained by the fact that some important information sits behind paywalls in databases that are commonly accessible to stakeholders in academia, but less so for other stakeholder groups. Yet there are also numerous free online databases that provide easy access to extensive information on the details of relevant laws and their application.[6] Ultimately, then, this aspect of the survey results partly highlights a need for capacity building.

In comments from surveyed and interviewed experts, it was clear that respondents were gaining a degree of access to relevant information, but in neither a consistent nor comprehensive manner. The lack of a single authoritative source, reliance on multiple (sectoral) newsletters, the lack of transparency, lacking online access, the use of legal jargon, and information overload were all mentioned as concerns. The broad scope of the topic may be a factor, as well. As made clear in Chapter Three, which examines topical trends, cross-border legal challenges on the internet arise in such a diverse range of substantive areas that it is extremely onerous and challenging to stay up-to-date.

It is noteworthy that the surveyed experts made no specific reference to academic writings as a source of information, suggesting that the work of academics does not effectively reach the other stakeholder groups. There would be significant value in exploring options for improving this currently lacking transfer of knowledge.

In enabling evidence-based policy innovation, this Report seeks to provide all stakeholders with the necessary information to develop frameworks and policy standards for the digital society and economy. It aims to give a comprehensive and regionally balanced overview and documentation of past, current and emerging trends, relevant actors and proposed solutions to the major cross-border legal policy challenges facing the connected society. In doing so, the Report accounts for the fact that the internet may be approached as: (a) a physical technical infrastructure (i.e., the hardware, routers, servers, computers, satellites, fiber optic cables, etc.); (b) a logical structure (i.e., the technical protocols that govern online interactions); and (c) a social construct made up of the available content and cyber activities. The Report complements the ongoing policy development process facilitated by the Secretariat of the Internet & Jurisdiction Policy Network. Thus, it builds upon the findings and issues addressed in the three thematic Programs of the Internet & Jurisdiction Policy Network, namely:

1. Data & Jurisdiction Program;
2. Content & Jurisdiction Program;
3. Domains & Jurisdiction Program.

The Report's topical coverage has been selected, and is limited, by reference to the Internet & Jurisdiction Policy Network's focus on internet governance at the intersection of the three areas of digital economy, human rights, and cybersecurity. Therefore, the coverage is not limited to questions of internet jurisdiction *per se*, but rather encompasses a broad range of procedural and substantive law issues falling within the broad topic of cross-border legal challenges facing the internet. Yet, the coverage is distinctly limited to these cross-border legal challenges and

> "The coverage is not limited to questions of internet jurisdiction per se, but rather encompasses a broad range of procedural and substantive law issues falling within the broad topic of cross-border legal challenges facing the internet."

5. One surveyed expert specifically referred to this resource: Global Forum for Media Development. *Internet Governance*. Retrieved from https://gfmd.info/internet-governance/.

6. Free Access to Law Movement. Retrieved from http://www.falm.info/members/current/.

does not aim to address general internet-related issues.

In alignment with the Internet & Jurisdiction Policy Network's focus areas, the Report addresses neither cyberwar, nor cyber conflict more broadly. At the same time, it is not always possible to distinguish activities that fit within the field of cyber conflict from those that do not, in the online environment. For example, cyber espionage is carried out for both military and economic purposes, and when it is directed at defense industries or critical infrastructure, distinguishing between military and non-military espionage may be virtually impossible; rather, such espionage activities are simultaneously military and non-military. Likewise, drawing a sharp line between national security information sharing and information sharing in the context of law enforcement is not always possible, either.

A significant number of stakeholders have called for a timely compendium of global activities. It is hoped that this Report – made possible by the strong support that the Internet & Jurisdiction Policy Network enjoys from its stakeholders – can meet that need and serve as a crucial instrument to help foster policy coherence across ongoing initiatives.

Thus, the Report stands to contribute to the mitigation of acute jurisdictional conflicts, to support the development of concrete operational solutions, and to preserve the benefits of the open, interoperable and cross-border internet.

1.2

Transnational as the new normal

The world consists of nearly 200 countries, some industrialized and some developing. All these countries have their own history, economy and cultures. They have different social structures, political systems and laws. Many are home to cultural diversity, and some have a diverse range of laws. The people who populate these countries are of different ethnicities, and they speak different languages. They hold different values, religious beliefs and political opinions. Indeed, even where they hold the same values as important, they frequently take different views on how those shared values should be balanced in specific cases where they clash with one another. This staggering diversity stands in contrast to the fact that we all – so far – essentially share one internet.

During interviews carried out in support of the Report drafting, the European Union's General Data Protection Regulation (GDPR), introduced in 2018, was by far the most frequently mentioned legal initiative. Few, if any, previous legislative initiatives have gained a similar degree of international attention. So why is it that one can speak to people from anywhere in the world and find that they are not only aware, but have detailed knowledge, of the GDPR – a law issued by lawmakers in Europe, far away from countries such as Australia, Brazil, China and the Democratic Republic of Congo? When the European Union introduced its Data Protection Directive in the mid-1990s, it gained only limited and sectoral international attention. What then changed in the world to render the GDPR a virtually ubiquitous topic of discussion?

The answer is probably twofold. First, globalization has changed the world since the mid-1990s, and the ecosystem is now more alert to how the laws of one jurisdiction can impact people in other parts of the world. This is an inescapable consequence of increased interconnectedness. Further, states are now more frequently looking to other states when seeking to shape their own legal responses to the challenges that stakeholders face. The internet has strongly contributed to these developments. Second, there is now considerably greater recognition of the role that data – and therefore, data privacy – plays in our lives. This change, too, has been predominantly driven by the internet.

> "Matters that were once determined domestically are now transnational in nature, necessitating a different mindset among decision makers on all levels."

The GDPR is merely one of many laws that impact individuals beyond their original jurisdiction. In fact, most countries' laws have such an impact on some level. As many interviewed experts observed, this makes for an increasingly complex regulatory environment.

The observation that the online environment is largely transnational may seem like little more than a truism; but this trend has profound implications, giving rise to problems and af-

fecting approaches to their solution. Several interviewed and surveyed experts noted that matters that were once determined domestically are now transnational in nature, necessitating a different mindset among decision makers on all levels. The stakes are high, and the diversity is great.

The importance of communication (including cross-border communication) is well-established; and no other medium can facilitate cross-border communication as fluidly as the internet. The online environment lends itself to the kind of cross-border communication that online communities in both industrialized and developing countries expect, and that can lead to cross-border disputes. Addressing transnational issues is, therefore, not optional, and the necessary internet jurisdiction rules must be able to cope with a high volume of disputes.

As an international environment, issues of internet regulation also require internationally oriented solutions; whether pursued on an international or domestic level, solutions must account for the international context in which they will operate. Both useful and harmful approaches are likely to have cross-border implications and may spread internationally. Kant's 'categorical imperative' comes to mind, prompting the pursuit of universal solutions.

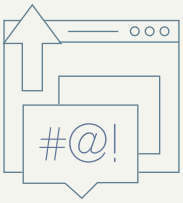
Unfortunately, the international political climate has recently changed. There is a significant move away from international collaborative efforts and common goals, as more states adopt inward-looking policies and put their own immediate interests first. Trust is being replaced by distrust, collaboration by the rule of the strongest. Such trends represent a substantial obstacle for the effective coordination of internet regulation. However, it remains an inescapable fact that cross-border legal challenges on the internet can only be addressed through international collaborative efforts and the pursuit of common goals; no state, company or organization can do this alone, and the ecosystem simply cannot afford not to collaborate.

> "Trust is being replaced by distrust, collaboration by the rule of the strongest."

1.3

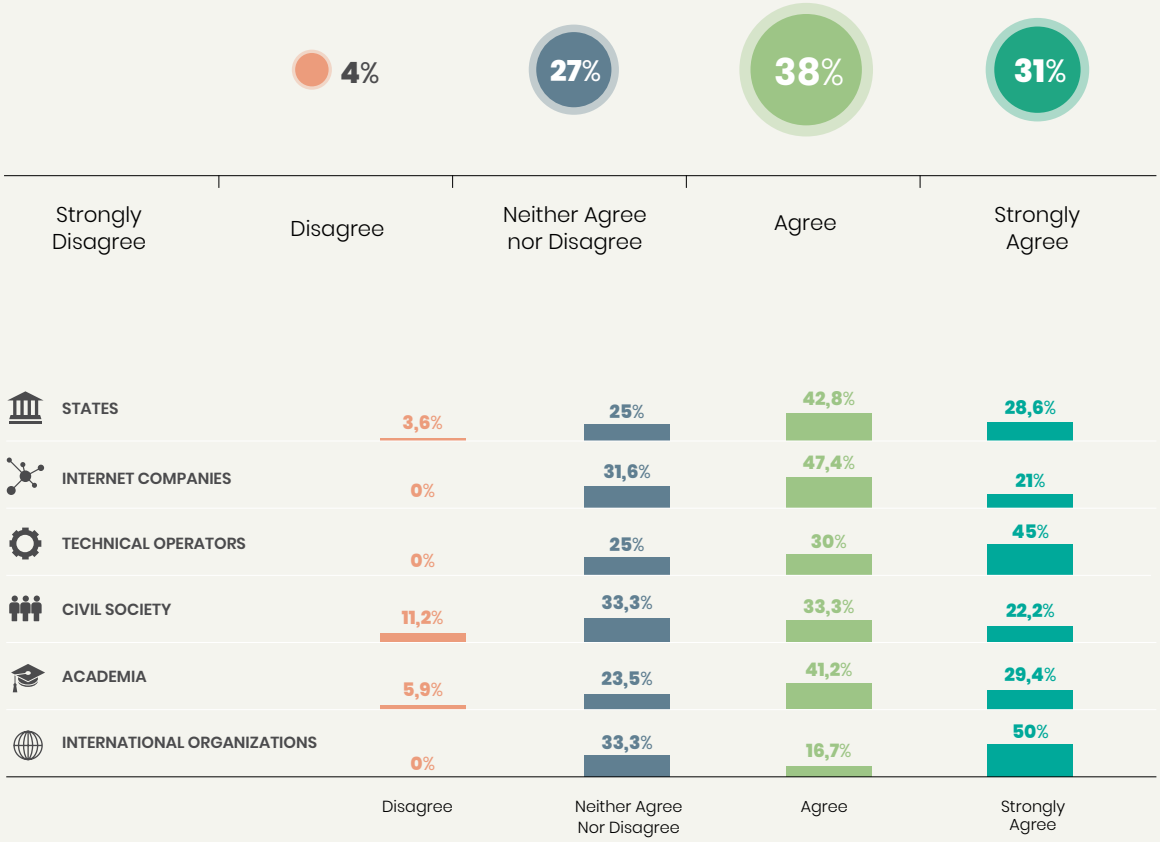
Growing concern over abuses

There is a general feeling among the Internet & Jurisdiction Policy Network's stakeholders that online abuse is increasing. A clear majority – 69% of surveyed experts – either 'agreed' or 'strongly agreed' that online abuses (e.g., in the form of hate speech, harassment, hacking, privacy violations, or fraud) are increasing. 27% 'neither agreed nor disagreed', and only 4% 'disagreed' or 'strongly disagreed'.



INFOGRAPHIC 3

Are online abuses, for example in the form of hate speech, harassment, hacking, privacy violations, or fraud, increasing?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Despite the agreement that online abuses (e.g., hate speech, harassment, hacking, privacy violations, or fraud) are increasing, the percentage of respondents that 'neither agreed nor disagreed' was substantial and many surveyed experts said the lack of empirical evidence made it difficult to answer this question.

This observation is both fair and important; and it reflects the sophistication of the ecosystem. It directs attention to the fact that there is currently a lack of reliable data, which, in turn, is linked to the need to standardize methods and initiatives to collect reliable data to inform policy decisions.

A recurring theme in comments made by surveyed experts is that while online abuses are increasing, so is the overall use of the internet – in other words, both abuse and normal use are increasing (possibly in proportion). One surveyed expert correctly pointed out that this is a question of percentages versus absolute numbers. With more people online, and more layers of services and platforms, the absolute volume of both online abuse and the people affected by it increase. Yet this is a separate matter to whether there is an increase in the percentage of people misbehaving out of the overall body of internet users. Some surveyed experts also noted that as awareness of online abuses has increased, so too has the willingness to report abuses.

Both these factors may contribute to a perception that online abuses are increasing. A key trend here is that increasing awareness of, and sensitivity to, these abuses result in increasing political pressure to address them. This political pressure risks sparking uncoordinated, unilateral reactions that do not achieve desirable long-term effects.

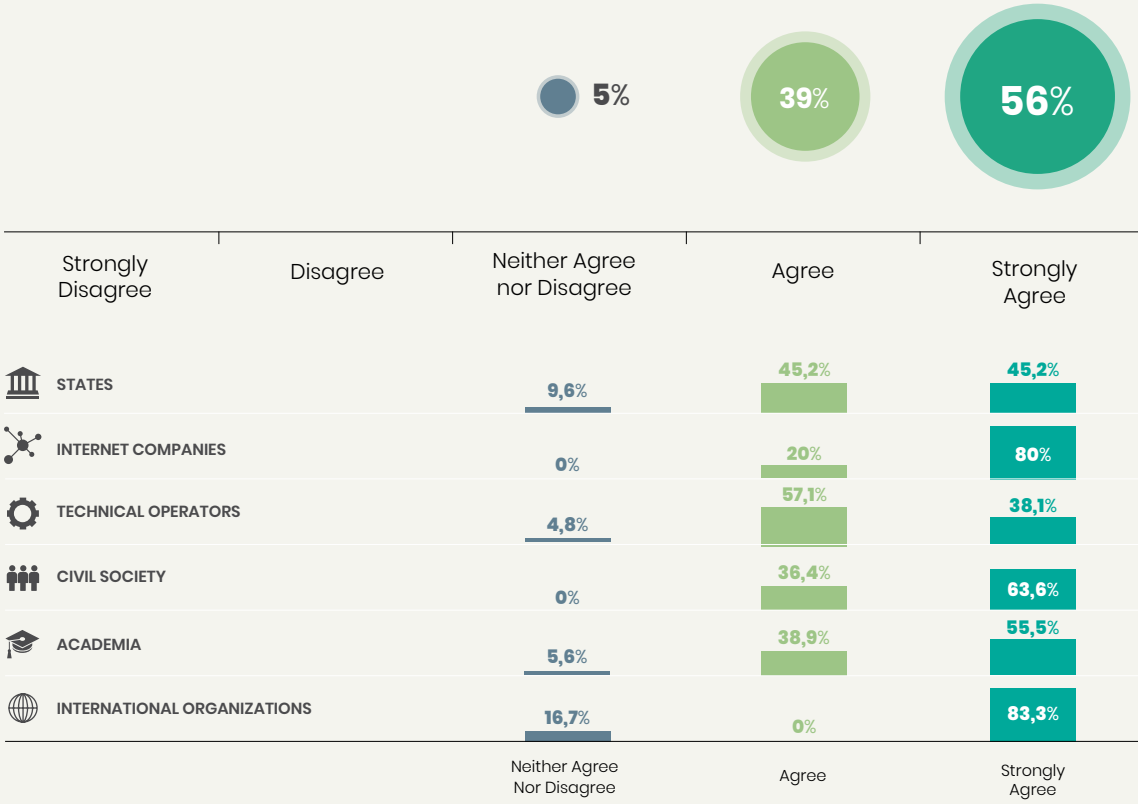
Some interviewed experts made the point that the internet merely mirrors conduct offline. One surveyed expert suggested that abuse is increasing both offline and online because of the current political and economic climate, and that online platforms simply reflect society. Yet different types of abuses also emerge online. The internet gives greater visibility to things that were once largely restricted to the private sphere and, therefore, makes it easier for them to spread.

Another interviewed expert emphasized that these dynamics differ across cultures, and that there are increasing differences in what is seen as harassment, privacy violations and hate speech.

A majority (56%) of surveyed experts 'strongly agreed' that the cross-border legal challenges on the internet will become increasingly acute in the next three years. A further 39% 'agreed' and none of the surveyed experts 'disagreed' or 'strongly disagreed', while 5% responded that they have no view on this question.

INFOGRAPHIC 4

Will cross-border legal challenges on the internet become increasingly acute in the next three years?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Comments provided by surveyed experts highlighted a widely held view that the combination of three factors will make cross-border legal challenges on the internet increasingly acute:

1. The world is increasingly becoming interconnected through the internet, thereby increasing diversity online;
2. The internet is deeply affecting societies and economies, meaning that the stakes are high; and
3. Nation states with different visions are seeking to increase their control over the internet, primarily by using national tools rather than transnational cooperation and coordination.

As one surveyed expert pointed out, in all this, the internet is neither the problem, nor the cause of the problem. Rather, the internet is the victim.

> "As one surveyed expert pointed out, in all this, the internet is neither the problem, nor the cause of the problem. Rather, the internet is the victim."

1.4

Competing legitimate interests need reconciling

A 'genuine regulatory challenge' exists where there are competing legitimate interests that are difficult to reconcile. In the context of internet jurisdiction, there are numerous instances of competing legitimate interests. For example, state A's protection of free speech may be difficult to reconcile with state B's restrictions on hate speech.

The genuine regulatory challenges facing the ecosystem can be boiled down to the need to reconcile, or at least balance, the three dimensions of:

1. fighting abuses;
2. protecting human rights; and
3. promoting the digital economy.

All three of these dimensions are strongly affected by two complicating factors of fundamental importance:

1. individual interests are being pursued at the expense of the common good; and
2. there are competing rationalities/visions for what is the common good.

To a great extent, the difficulties in finding solutions to cross-border legal challenges on the internet stem from the fact that the genuine regulatory challenges are numerous and involve legal notions that are central to the identity of individual states. Yet, this does not fully explain the complexity of the situation facing the ecosystem. Some of the challenges stem instead from the inadequacy of the legal concepts used.

1.5

Existing legal concepts are under stress

Most legal concepts with which we work – such as the focus on the location of evidence – were developed in the offline context.

The application online of pre-internet legal concepts often involves decisions on the appropriate analogies and metaphors. The impact of such decisions was famously highlighted in the mid-1990s during the debate over the constitutionality of the US Communication Decency Act (CDA),[7] and was again on display in the 2016 Supreme Court of Canada hearing in the *Equustek* case.[8] Representing Google Inc, McDowell suggested that, Google search was akin to a librarian that managed one of several card catalogues. In contrast, Justice Karakatsanis suggested a different analogy, comparing Google search to the person behind the counter of a bookstore. The choice of analogy would clearly impact the question of responsibility.

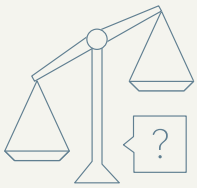
Several interviewed experts emphasized the concern that, in the jurisdiction field, legal concepts are old fashioned and outdated. This creates 'artificial regulatory challenges' in that the frameworks and concepts being applied are insufficient to address the issues; in other words, the inadequacy of the tools may cause regulatory challenges. This prevents, or at least limits, progress.

Perhaps the most central concept under stress is the binary distinction between territorial and extraterritorial. While it – like other binary simplifications, such as the distinction between day and night – may work for certain purposes, they are inadequate for other important purposes. Much like the failure of the day/night distinction to take into account dusk and dawn, and indeed the many nuances between, viewing the strength of jurisdictional claims from the binary perspective of territorial versus extraterritorial does not adequately reflect the nuances involved.

---

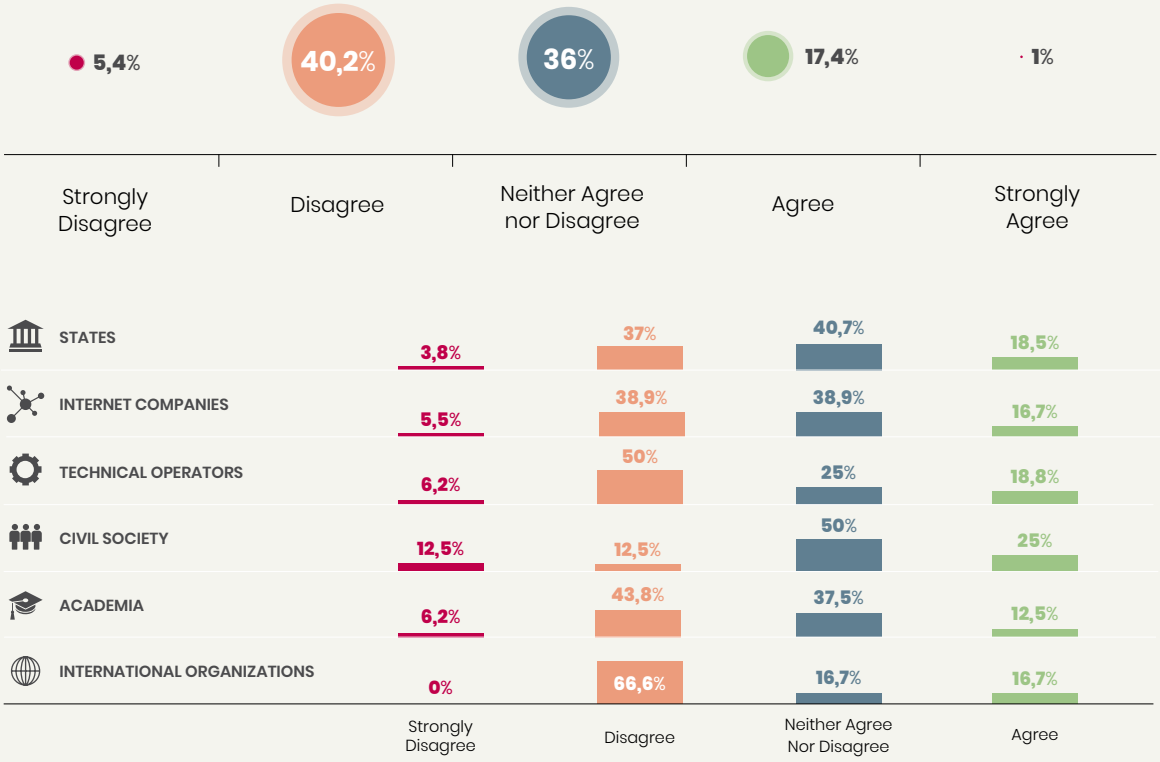
7. Webach, K. (1997). Digital tornado: The internet and telecommunications policy. (Working paper of the Federal Communications Commission). Retrieved from https://www.fcc.gov/reports-research/working-papers/digital-tornado-internet-and-telecommunications-policy.

8. Google Inc v Equustek Solutions Inc 2017 SCC 34. Retrieved from https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.



INFOGRAPHIC 5

Are we already applying the right legal concepts to address cross-border legal challenges on the Internet?



SOURCE; Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Concerns about legal concepts

One of the survey questions posed the claim that we already apply the right legal concepts to address cross-border legal challenges on the internet. Among the surveyed experts, 46% either disagreed or strongly disagreed, 36% indicated that they neither agreed nor disagreed, and 18% either agreed or strongly agreed. Comments from the surveyed experts offer guidance as to how these statistics should be understood, and what the concerns are. For example, one surveyed expert qualified their agreement with the above claim by stressing that, although the basic legal concepts are sound and relevant, their application to the online environment remains a challenge. This concern is also recurring in the literature.

Another surveyed expert noted that there are several lacunae in the legal concepts, and yet another emphasized that there is a categorically new challenge in melding the global internet with national borders, and that we do not have the right legal concepts or principles for this task. The latter surveyed expert also made the point that this challenge is more complicated than other cross-border challenges, such as the regulation of financial transactions or airspace.

These survey responses correspond to observations commonly made in the literature. For example, the mobility of data undermines the utility of several traditional jurisdictional anchor points.

A related concern is that arguably too much of the discussion around cross-border legal challenges on the internet relies on legal concepts involving imprecise abstractions that are difficult to operationalize. In part, this is due to differing understandings of fundamental legal concepts. One example of this is found in the term 'comity,' which has a quite specific meaning in US law but remains a vague and controversial concept in international law. Due to the variations in legal systems around the world, one surveyed expert noted that, it might be difficult to even assert which are the 'right legal concepts'. Another surveyed expert pointed out that while some regions of the world work with the 'right' legal concepts, we do not do so on a global level.

One surveyed expert noted that courts lack the right black letter law framework. However, the same expert also added that arriving at the right black letter law framework would not be so difficult and would not require any major reinvention of the law.

In this context, a potential barrier is the degree to which courts properly understand and keep up with technological developments. Once, this challenge was openly acknowledged by the courts. Most famously, in 1997, the US District Court for the Southern District of New York observed that: "Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average [...] five-year-old tosses about with breezy familiarity."[9] Today, one rarely sees such open admissions. Yet, while the judiciary's general IT competence doubtlessly has increased over the years, it may be suggested that the complexity of relevant technologies has increased at an even faster pace. Thus, the question of whether we are in a better position or not than we were in 1997, when the US District Court for the Southern District of New York made its observation, has no obvious answer.

At any rate, due to the complexity involved, few areas are as plagued by artificial regulatory challenges as the debate about cross-border legal challenges on the internet. One need only consider the conceptual complexity involved in analyzing a standard cross-border legal issue, such as a claim of jurisdiction over conduct that occurs in another state but affects the state making the claim. In such a situation, tradition would dictate beginning with a consideration of whether the matter falls within public or private international law – a question that does not always have an obvious answer.[10]

If the matter falls under private international law, there is a need to consider other matters, such as whether there are grounds for claiming personal jurisdiction and subject matter jurisdiction. Then, there is a need to identify the applicable law and determine whether there are any grounds for the court in question to decline to exercise jurisdiction. Only then can the matter be heard. Once a judgment is issued, new issues arise around recognition and enforcement.

On the other hand, if the matter falls under public international law, tradition points to at least three different types of jurisdic- tion for consideration – prescriptive, adjudicative and enforcement jurisdic- tion, to which a fourth (investigative jurisdiction) has recently been added. Each of these types of jurisdiction is associated with unclear and vague criteria, and it is not always obvious to which category a given matter would belong. For prescriptive jurisdiction, there is a set of commonly referenced principles known as the *Harvard Draft Principles*[11], with the addition of the so-called 'effects doctrine'. These principles were originally drafted for a narrower purpose compared to how they are often treated today. The criteria are less clear for adjudicative and enforcement jurisdiction, however, and the detailed criteria for investigative jurisdiction remain to be defined.

If the claim of jurisdiction overcomes these hurdles, there are still numerous other considerations, such as:

- Would the claim of jurisdiction violate the sovereignty of another state (assuming sovereignty remains viewed as a right on its own that can be violated)[12]
- Would the claim of jurisdiction be contrary to the duty of non-intervention?
- Would the claim of jurisdiction be contrary to comity?
- Is the claim of jurisdiction in fact mandated by the due diligence principle? [13]

The conceptual complexity works as a barrier to entry, preventing the 'uninitiated' from contributing to the debate, and risks making this field the exclusive domain of a small group of specialist lawyers. It also regularly results in misunderstandings and miscommunication. Furthermore, it creates an environment in which discussions are characterized by overly broad and simplistic claims, leading to locked positions; too often, the legal concepts are not debated in a systematic manner. Instead, there is a tendency to pick and choose concepts that support any given position.

---

9. American Libraries Association v Pataki 1997 SDNY 969 F Supp 160, 170 (per Preska J).

10. Or 'conflict of laws' as 'private international law' often is referred to in Common Law countries.

11. Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935. (1935). Supplement *American Journal of International Law*, 29, 443, p. 445.

12. (2017). Sovereignty, cyberspace and Tallinn manual 2.0. *American Journal of International Law Unbound*, 111. Retrieved from https://www.cambridge.org/core/journals/american-journal-of-international-law/ajil-unbound-by-symposium/sovereignty-cyberspace-and-tallinn-manual-2-0.

13. See Chapter 5 'Relevant concept clusters 101' for definitions of these concepts.

A proponent of a claim of jurisdiction may, for example, feel vindicated by the 'effects doctrine' (while ignoring all other principles), while an opponent to the same claim may feel vindicated by the 'comity principle' (while ignoring all other principles). The complexity may hide the flaws in their respective approaches, and because they both feel supported by law, the likelihood of agreement – or even of a constructive discussion – is low. This highlights a clear need for a simpler legal framework of foundational principles in which to anchor the discussion. The Report points to a possible overarching jurisprudential framework for jurisdiction in which attention is directed at three criteria:

1. whether there is a substantial connection between the matter and the state seeking to exercise jurisdiction;
2. whether the state seeking to exercise jurisdiction has a legitimate interest in the matter; and
3. whether the exercise of jurisdiction is reasonable given the balance between the state's legitimate interests and other interests.

These criteria are gaining increasing recognition[14] and transcend the perceived gap between public and private law. Further, they incorporate both effects doctrine and comity, as well as other relevant public and private international law concepts. As such, they amount to a suitable foundation upon which to build more detailed legal norms for specific contexts.

Current discussions of cross-border legal challenges on the internet predominantly focus on tackling the most pressing day-to-day issues (i.e., some of the genuine regulatory challenges), at the expense of focusing on the underlying conceptual complexity (i.e., the artificial regulatory challenges). This is natural, given the impact that these challenges have for society. However, real progress can only be made if the ecosystem also tackles the artificial regulatory challenges. Indeed, the artificial regulatory challenges must first be addressed in order to adequately address the genuine regulatory challenges. It is hoped that this Report can contribute to this important task.

To this end, the subsequent Chapters of this Report take care to not only engage with and outline the genuine regulatory challenges, but to do so in a manner that may mitigate some of the artificial regulatory challenges alluded to here.

"Current discussions of cross-border legal challenges on the internet predominantly focus on tackling the most pressing day-to-day issues (i.e., some of the genuine regulatory challenges), at the expense of focusing on the underlying conceptual complexity (i.e., the artificial regulatory challenges)."

14. United Nations Special Rapporteur on the Right to Privacy Task Force on Health Data. (2019). *Draft recommendation on the protection and use of health-related data.* Retrieved from https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf.

1.6

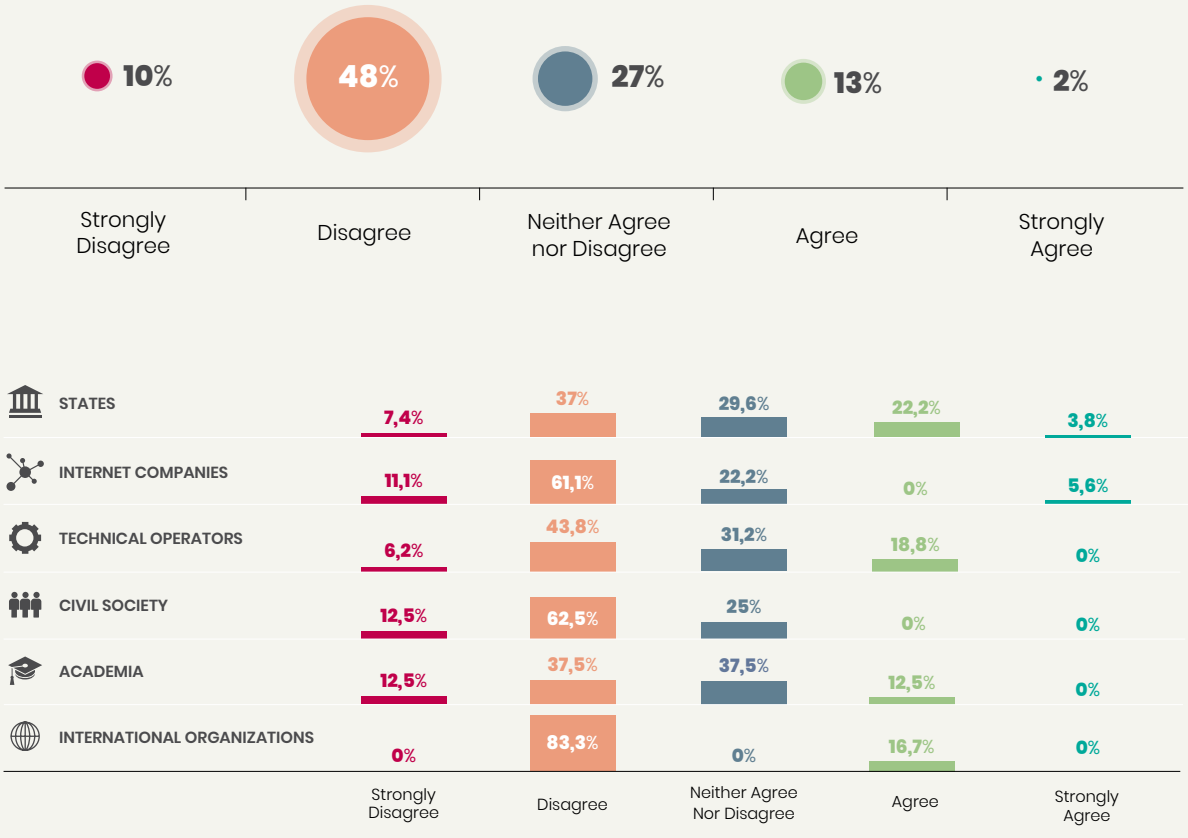
Proper frameworks and institutions are lacking

The Internet & Jurisdiction Policy Network's stakeholders pointed to a current lack of appropriate institutions to address cross-border legal challenges on the internet.

The majority (58%) of surveyed experts either 'disagreed' or 'strongly disagreed' that we already have the right institutions in place to address cross-border legal challenges on the internet. Only 15% of surveyed experts stated either 'agreed' or 'strongly agreed', while 27% indicated that they neither 'agreed' nor 'disagreed'.

INFOGRAPHIC 6

Do we have the right institutions to address cross-border legal challenges on the internet?



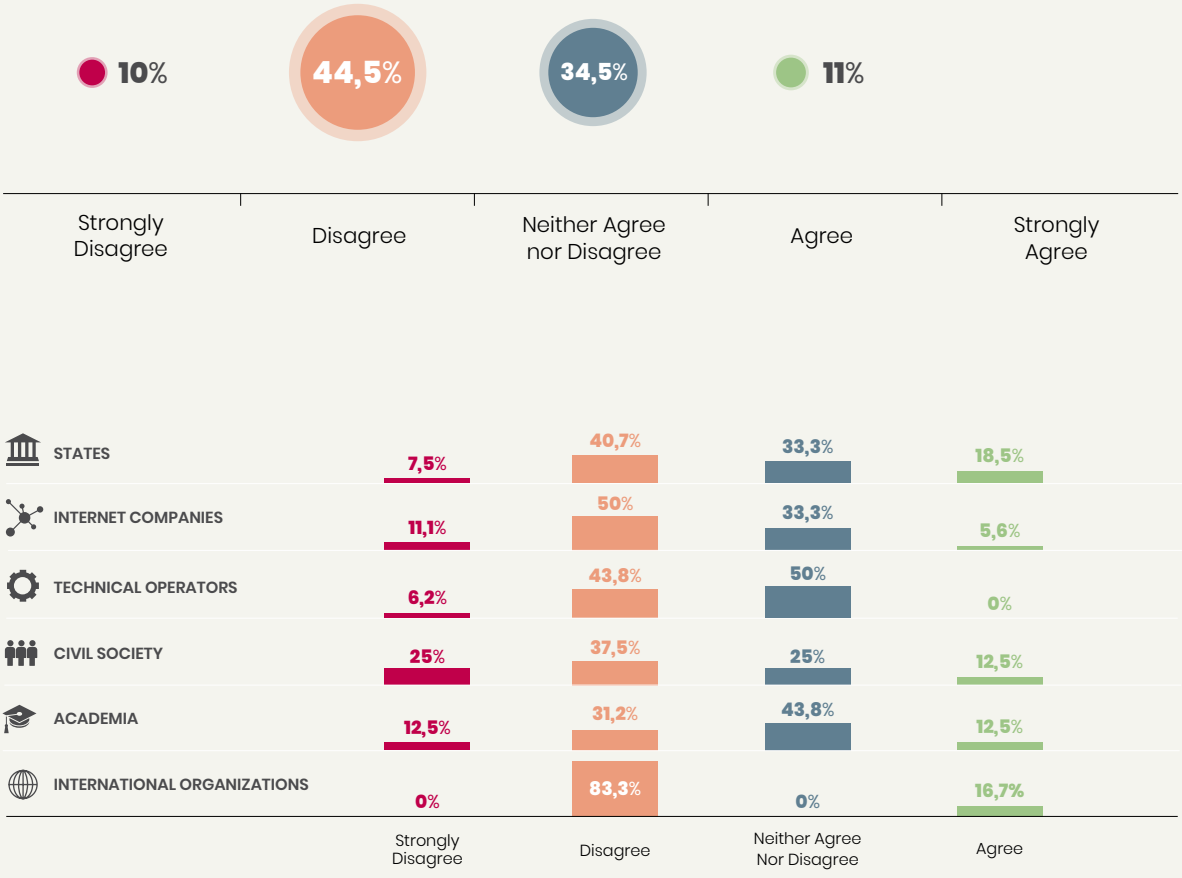
SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Some surveyed experts commented that awareness of the sensitivity of cross-border legal challenges on the internet is often low in current institutions – both internationally and domestically – and that they need to evolve and better cooperate with one another. Among surveyed and interviewed experts, there was a clear majority view that although numerous institutions work on these issues, additional fora or institutions might be beneficial. A smaller number expressely doubted the need for additional institutions.

Another aspect of lacking coordination relates to the availability of appropriate frameworks and standards. 44.5% of surveyed experts 'disagreed', and a further 10% 'strongly disagreed', with the assertion that we have the frameworks and standards to address cross-border legal challenges on the internet. Only 11% of surveyed experts 'agreed', and none 'strongly agreed'. 34.5% of surveyed experts indicated that they neither 'agreed' nor 'disagreed'.

INFOGRAPHIC 7

Do we have the right frameworks and standards to address cross-border legal challenges on the internet?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

In their comments, surveyed experts pointed to regional differences, with some noting that global standards do not exist and are unachievable. Others pointed out that the cross-border legal challenges on the internet are being addressed under ordinary domestic laws, with some adding that many cross-border challenges cannot effectively be addressed within the national domain.

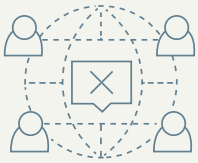
The survey highlights that:

1. states are attempting to address the cross border legal challenges on the internet by applying their existing laws;
2. but national responses are inadequate; and therefore,
3. there is a clear need for transnational coordination and cooperation.

1.7
Coordination is insufficient

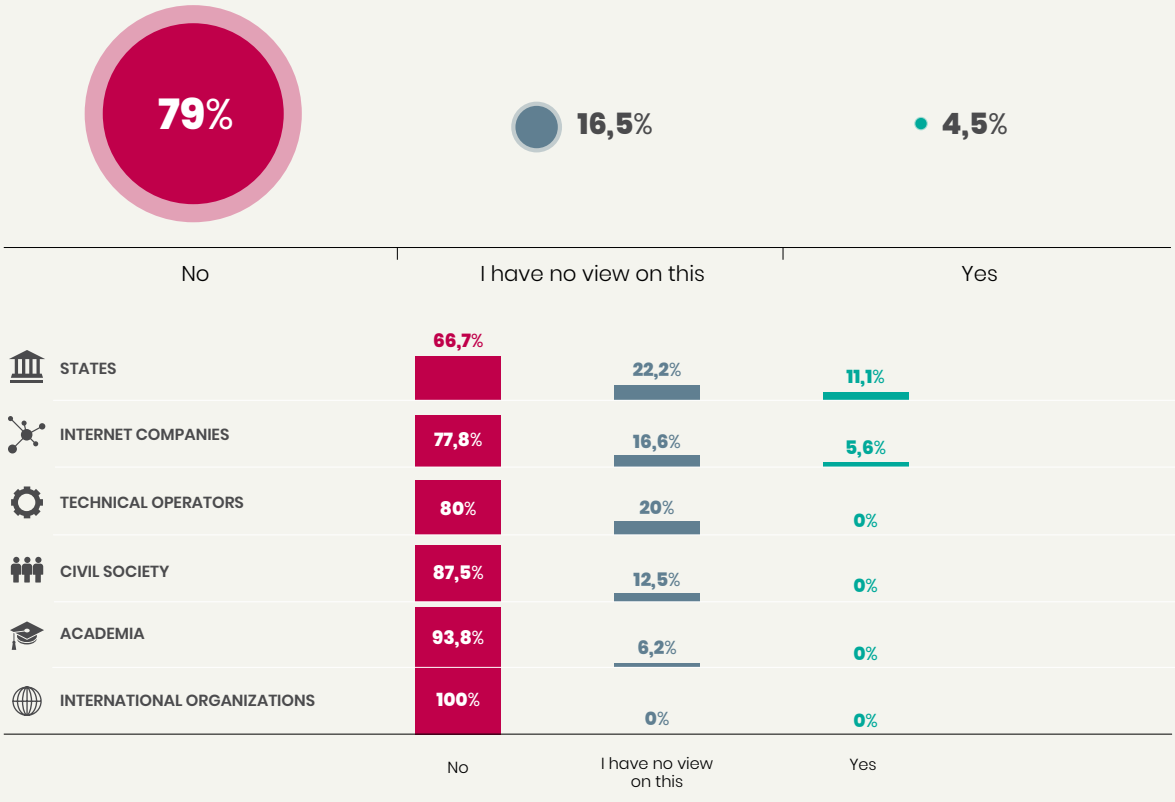
The stakeholders sent a strong message that current coordination efforts are insufficient.

When asked whether there is sufficient international coordination and coherence to address cross-border legal challenges on the internet, no less than 79% of surveyed experts answered 'no', while only 4.5% answered 'yes'. 16.5% responded that they have no view on this question.



INFOGRAPHIC 8

Is there sufficient international coordination and coherence to address cross-border legal challenges on the Internet?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

While the survey results shows a clear and overwhelming consensus across stakeholder groups and regions, it should be noted that some surveyed experts said robust international coordination and cooperation can be seen among certain groups and in certain sectors. One example mentioned was coordination among law enforcement agencies, e.g., via the work of Interpol, Europol and the Council of Europe.

1.8

Fundamental attributes of the internet are at stake

Should the internet be preserved? While the vagueness of this question is obvious, the instinctive answer is probably still a resounding 'yes'. After all, the internet has already revolutionized how people, businesses and governments interact; it plays a central role in the lives of billions of people, and has brought numerous significant economical and societal benefits.

While there is seemingly clear support for preserving the internet as we know it, it is also widely recognized that the internet is constantly evolving. This is perhaps particularly true in the global south, where the internet's uptake, structure and usage are evolving quickly. As the way we use the internet has changed over the years, so too has the content available online and the internet's technical infrastructure. Online, change is constant and natural, and it typically translates into desirable progress.

Nevertheless, there are perhaps certain characteristics of the internet that ought to be shielded against change. If so, what might those characteristics be? What is it about the internet that instinctively deserves to be preserved? These kinds of questions may be answered at different levels of abstraction. At a relatively high level, one might point to the internet's openness, and its role as an enabler and protector of human rights and democratic values, as qualities that are particularly worth preserving. Other such qualities include the internet's potential to contribute to a fairer and more equitable world, and to bring people closer together through a global communications medium, ultimately supporting a peaceful coexistence.

Unfortunately, all these characteristics are currently under threat, to varying degrees, and they cannot be taken for granted. Rather, it must be recognized that the internet is a fragile environment and that the characteristics of the internet that are to be preserved must be actively protected. Two such characteristics are the internet's cross-border and permission-less nature – both of which are under threat.

> "The characteristics of the internet that are to be preserved must be actively protected."

1.8.1

The cross-border internet cannot be taken for granted

As noted in a brief September 2018 Internet Society concept note on the internet and extraterritorial effects of laws: "Globalization is a feature of the internet, not a bug, and legal systems everywhere should recognize this, not try to 'fix' it."[15] This observation is both accurate and important. Yet, as discussed in detail below, the regulatory landscape online (and offline) has always been fragmented. This is a direct consequence of the sovereignty that states enjoy, insofar as they have the capacity to make their own laws. Indeed, it has been noted that the difficulty of applying and enforcing any regulatory system online may be attributed to the fact that the internet's

15. Internet Society. (2018, September). *The internet and extra-territorial effects of laws*. Retrieved from https://www.internetsociety.org/wpcontent/uploads/2018/10/The-internet-and-extra-territorial-application-of-laws-EN.pdf, p. 1.

operation involves a highly fragmented universe of actors, norms, procedures, processes and institutions, including many non-state entities.[16]

Although this kind of fragmentation is nothing new in the online ecosystem, states are making increasingly aggressive jurisdictional claims and backing up those claims with heavy fines or even the threat of imprisonment (Chapter 4.1.2), raising the stakes for the subjects of regulations. Therefore, both natural and legal persons may opt to avoid having an online presence on certain markets. For example, those wishing to avoid contact with certain states may utilize technical measures such as geo-location technologies (Chapter 4.2.1), or non-technical measures such as disclaimers or terms of service excluding access based on location.

Whether technical or non-technical, this type of fragmentation – if widespread – is a threat to the cross-border internet and carries both societal and economic consequences. Fragmentation online contributes to fragmentation offline, resulting in a loss of some useful interactions and cross-border engagements that may spark mutual trust and understanding. As to the financial side, it has been noted that: "The balkanization of the internet will change how companies do business. This will likely reduce efficiency and, in a macro way, have some effect on the global economy."[17]

At the same time, it may be argued that some degree of fragmentation is the only way to uphold national rules – which may be necessary to avoid a lawless internet – and avoid claims of global jurisdiction (Chapters 3.1.2.1, 3.1.6.2 and 4.1.7). The task, then, is to determine the type and degree of acceptable fragmentation, without endangering the characteristics of the internet that should be shielded from change.

In a sense, what we are witnessing is a decreasing gap between the initially borderless internet and the territorially grounded legal systems; the internet is becoming less 'borderless', and legal systems are becoming less anchored in territoriality. If properly coordinated and managed, this development stands to provide great benefits to both the fight against abuses and the protection of human rights, as well as the digital economy. If mismanaged, however, it may spell disaster for the online environment.

---

16. Kuner, C. (2017, February 1). The internet and the global reach of EU Law. *Law Society Economy Working Papers* No. 4/2017. Retrieved from SSRN: https://ssrn.com/abstract=2890930 or http://dx.doi.org/10.2139/ssrn.2890930, p. 7.

17. PwC. (2018). *Revitalizing privacy and trust in a data-driven world.* Retrieved from privacy-trust-in-data-driven-world.pdf.

Fragmentation also occurs in a more technical sense. A useful distinction has been made between fragmentation on the internet, as discussed above, and fragmentation of the internet – fragmentation of the internet's underlying physical and logical infrastructures.[18]

The physical backbone of fiber optic cables crossing oceans and international borders enables a relatively seamless online experience regardless of location. Traditionally, these cables have been controlled by telecommunications operators, but a shift in ownership has given rise to at least two 'new' types of owners. The first is the major internet companies. Some of these companies have invested in their own trans-oceanic cables, resulting in private networks that connect their data centers and operate outside of the rules that have governed the internet and its network operators to date, such as those pertaining to common carriage and neutrality.[19]

The second category of new cable owners includes nation states seeking to pursue geo-political cyber strategies. China, most notably, is making significant investments to build a geographically strategic infrastructure that allows data to flow around the world entirely on Chinese-owned fiber optic infrastructure.[20] Such a nation-controlled infrastructure may be applied in order to reduce access to information, limit participation in online forums, restrict data privacy and freedom of expression, and perhaps embed surveillance and censorship capabilities.[21] These developments could be seen as a logical extension of the Great Firewall of China (Chapter 4.2.2), and may in fact make the current Great Firewall of China redundant. At any rate, they represent a serious attack on the neutrality of the internet's core infrastructure. Furthermore, they represent a step away from the internet as a 'network of networks' – a key feature that encourages a multistakeholder approach to internet governance – and pose a threat to the cross-border internet.

Another technological development that may lead to fragmentation is exemplified in the Russian government's ambitions to develop a separate back-up of system of Domain Name Servers (DNS), which, according to 2017 reports, would not be subject to control by international organizations.[22] The Press Secretary of the Russian Presidency has specified that Russia does not intend to disconnect from the global internet, arguing instead that recent unpredictability from the US and EU demanded that Russia be prepared for any turn of events.[23] On February 11, 2019, it was reported that Russia has taken several major steps in this direction.[24]

In May 2019, Russia's internet sovereignty law was reportedly signed by Vladimir Putin creating an isolated domestic internet network.[25]

Furthermore, major satellite-based internet connectivity, while largely in its infancy, may have the potential to facilitate and accelerate fragmentation of the internet.

In a sense, the fragmentation of technical infrastructure likely poses a greater threat to the global internet than fragmentation arising from the regulatory landscape online. Moreover, while there is a degree of political will to attempt to overcome the negative effects of fragmentation sparked by regulatory challenges, there are currently no signs of any developments that may prevent or even slow down the fragmentation of technical infrastructure.

In tackling these issues, it is essential to keep in mind that the cross-border internet cannot be taken for granted; it is a resource that needs to be actively protected. Indeed, the cross-border internet – both from a technical and regulatory perspective – is a sensitive and fragile environment comprising multiple stakeholders and actors; changes for one stakeholder group may have potentially irreversible flow-on consequences for others.

---

18. World Economic Forum. (2016). *Internet fragmentation: An overview*. Retrieved from http://www3.weforum.org/docs/WEF_FII_internet_Fragmentation_An_Overview_2016.pdf, p. 3.

19. Song, S. Internet drift: How the internet is likely to splinter and fracture. *Digital Freedom Fund*. Retrieved from https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

20. Song, S. Internet drift: How the internet is likely to splinter and fracture. *Digital Freedom Fund*. Retrieved from https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

21. Song, S. Internet drift: How the internet is likely to splinter and fracture. *Digital Freedom Fund*. Retrieved from https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

22. Internet & Jurisdiction Policy Network. (2017, December). Russia reportedly moves ahead with plan to create independent DNS backup for BRICS countries. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6626_2017-12.

23. RT. (2018, February 20). *Russia to launch 'independent internet' for BRICS nations - report*. Retrieved from https://www.rt.com/politics/411156-russia-to-launch-independent-internet/.

24. Cimpanu, C. (2019, February 11). Russia to disconnect from the internet as part of a planned test. *ZD Net*. Retrieved from https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/.

25. Internet & Jurisdiction Policy Network. (2019, May). Russia's Internet Sovereignty law is signed into law. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTktMDUifQ==.

1.8.2

The permission-less nature of the internet needs active protection

A distinctive feature of the online environment is its permission-less nature. In setting up a website, for example, one may be responsible and liable for that website, but no permission is required to launch it. By removing barriers to entry, the permission-less nature of the online environment has been a great facilitator of innovation, and its importance is widely recognized. One of the NETmundial principles articulates this importance:

"The ability to innovate and create has been at the heart of the remarkable growth of the internet and it has brought great value to the global society. For the preservation of its dynamism, internet governance must continue to allow permission-less innovation through an enabling internet environment, consistent with other principles in this document. Enterprise and investment in infrastructure are essential components of an enabling environment."[26]

The EU's e-commerce Directive from 2000 includes another articulation of the permission-less nature of the online environment. Article 4(1) emphasizes that: "Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect."[27]

The fact that the internet, by tradition, has been a network of networks without a central authority has assisted – or even necessitated – the permission-less nature discussed here. However, with the move toward infrastructure-level fragmentation, the permission-less nature cannot be taken for granted in the future. Rather, it must be actively protected and preserved.

In addition, all the reasons the 'first generation regulators' felt so strongly about enshrining the permission-less nature of the online environment must be kept in mind in our current era of 'hyperregulation' (Chapter 2.2.2). Where the regulatory complexity creates a substantial barrier for innovative new actors entering the market, the permission-less nature of the online environment is arguably undermined.

> "With the move toward infrastructure-level fragmentation, the permission-less nature cannot be taken for granted in the future"

26. NETmundial Initiative. *The NETMundial Principles*. Retrieved from https://netmundial.org/principles.

27. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Article 4(1). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN.

1.9

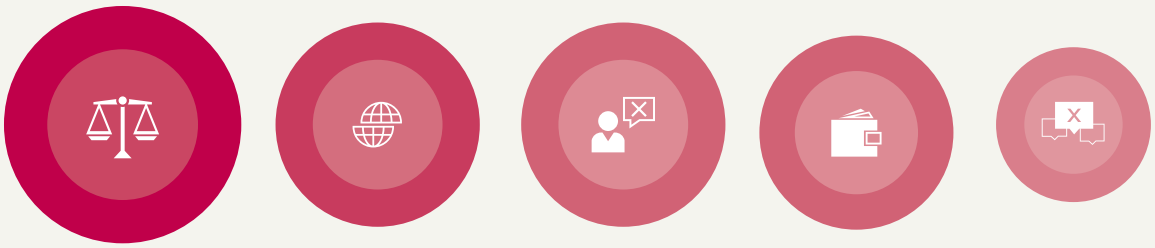
Not addressing jurisdictional challenges comes at a high cost

A failure to properly address the cross-border legal challenges on the internet will result in high costs for all stakeholders and may cause irreparable harm. Such negative consequences were highlighted in surveys and interviews.

When asked what, if any, negative consequences they foresee if cross-border legal challenges on the internet are not properly addressed, the Internet & Jurisdiction Policy Network's stakeholders highlighted the following in particular:

INFOGRAPHIC 9

What negative consequences, if any, do you foresee if cross-border legal challenges on the Internet are not properly addressed?



60% Legal Uncertainty

54% Loss of some key cross-border benefits of the Internet

54% Restrictions of expression

52% Compliance costs for online businesses

35% Inability to address online abuses

Top 5 answers by respondents

SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

In their comments, surveyed experts also identified the lack of rules to govern conduct on the internet as a risk. As one surveyed expert noted, as in every game with no rules, it is the strongest that will prevail.

1.10

A multistakeholder approach is still desired

The joint management of internet resources by governments, business and civil society in their respective roles – i.e., multistakeholderism[28] – remains the preferred approach to addressing cross-border challenges on the internet[29]. This was a clear theme among surveyed and interviewed experts.

Many interviewed experts pointed to multistakeholder models currently operating in certain spaces, such as governments working with social media companies in a collaborative or cooperative approach to combat issues like child abuse material or extremist activity online. Some specific examples cited include the activities of Internet Corporation for Assigned Names and Numbers (ICANN) [30] and the associated Regional At-Large Organizations,[31] the World Wide Web Consortium (W3C)[32] and the Internet Governance Forum (IGF), including its regional initiatives.[33] However, interviewed experts considered that there must be more robust interaction across more areas. For example, one interviewed expert said civil society and citizens must have a stronger voice in these discussions. Another interviewed expert stressed the importance of a multistakeholder model that incorporates industry agreement, as opposed to absolute oversight by government – an agile and flexible system that can allow issues to be addressed as they arise.

Another expert commented that we are seeing threats or attempts to undermine the multistakeholder approach, particularly due to unilateral initiatives from governments and private sector actors driven by their own national or commercial interests.

Thus, the message was clear that while a multistakeholder approach is still desired, the multistakeholder model is yet to be perfected and is facing competition from the mentioned unilateral initiatives.

Additionally, some interviewed experts pointed to an important gap in the widespread reliance on multistakeholderism. Court decisions have a significant impact on all cross-border legal issues on the internet. Yet, by their nature, court decisions are not reached through any process that may be described as multistakeholderism. Typically, only parties to the dispute are allowed to present arguments to the court. There is, therefore, an obvious risk that important interests are unrepresented at trials and overlooked by courts.

> "The message was clear that while a multistakeholder approach is still desired, the multistakeholder model is yet to be perfected and is facing competition from [...] unilateral initiatives."

28. See e.g.: UNESCO. (2017). *What if we all governed the internet? Advancing multistakeholder participation in internet governance*. Retrieved from https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf.

29. For a 2019 example, see: GSMA. *Digital Declaration*. Retrieved from https://www.gsma.com/betterfuture/digitaldeclaration.

30. For a detailed discussion of ICANN's structure, see e.g.: Mahler, T. (2019). *Generic top-level domains – A study of transnational private regulation*. Cheltenham, United Kingdom: Edward Elgar Publishing; Bygrave, L.A. (2015). *Internet governance by contract*. Oxford, United Kingdom: Oxford University Press, Chapter 4.

31. For example, the African Regional At-Large Organization, the Asian, Australasian and Pacific Islands Regional At-Large Organization, the European Regional At-Large Organization, the Latin American and Caribbean Islands Regional At-Large Organization and the North American Regional At-Large Organization.

32. World Wide Web Consortium. Retrieved from http://www.w3.org/Consortium/.

33. For example, the Latin America and Caribbean IGF, East Africa IGF, Central Africa IGF, North Africa IGF, West Africa IGF, Central Asia IGF, Asia Pacific IGF and Arab IGF.

To address this weakness in the judicial system, some courts allow the filing of so-called *amicus curiae* – 'friend of the court' – briefs. Courts have allowed a large number of *amicus* briefs in some recent high-profile internet jurisdiction cases, such as the *Microsoft Warrant case*[34] heard in the US Supreme Court in February 2018.

From an international perspective, though, such accommodation of *amicus* briefs is an exception and most courts avoid non-party input, by: (1) not allowing *amicus* briefs at all, (2) adopting court rules that exclude *amicus* briefs in all but the most exceptional circumstances, or (3) interpreting the court rules restrictively to exclude non-party input. Restrictive approaches toward *amicus* briefs may be justified by the risk of delays and added costs. These are legitimate concerns, and courts are typically restrictive when it comes to amicus briefs, particularly those filed by foreigners. At the same time, though, the stakes are often high for non-parties, as well, including foreign non-parties.[35] In cases where courts feel empowered to make decisions with international impact, one may argue that they should accept the responsibility of ensuring that they are sufficiently exposed to the international interests that stand to be impacted by their decisions.

Against this background, reform of the *amicus curiae* system is arguably the most urgently needed enhancement of effective multistakeholderism.

1.11

A pressing challenge, insufficiently addressed

The cross-border legal challenges facing the internet are currently getting more attention in media and in policy discussions than ever before.

In many ways, the challenges faced in the context of internet jurisdiction are akin to the challenges the world is facing with climate change. Both challenges can only be addressed through cross-border cooperation and coordination, and both have a global impact that affects developing countries most acutely. Both challenges are also of a nature that might make individuals (and even individual states) feel unable to do anything of impact on their own to affect change. Yet another similarity is found in the enormous economic and societal implications at stake.

There are also important differences between the respective crises unfolding in the natural environment and the online environment. For example, while short-term economic arguments are often levied against proposals for decisive action against climate change, there are few, if any, economic arguments against tackling the cross-border legal challenges on the internet. On the contrary, decisive action against the cross-border legal challenges on the internet will also be rewarded economically in the short-term, not just in the long-term. Furthermore, while there are still climate change deniers, few doubt or even question the very real and negative impact of not addressing the cross-border legal challenges on the internet. More broadly, while it has been suggested that some states prefer to operate with an unclear and chaotic legal framework regarding matters, such as cyber espionage and cyber aggression, there are few that benefit from jurisdictional chaos and 'hyperregulation' online (Chapter 2.2.2). These latter points suggest that there ought to be a clear political will, and unquestioned economic and social justifications, to decisively tackle the challenges faced in the context of internet jurisdiction.

---

34. Wikipedia. Microsoft Corp. v United States. Retrieved from https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States.

35. Consider e.g., the Supreme Court of Canada's approach to *amicus* briefs in *Google Inc. v. Equustek Solutions Inc*. 2017 SCC 34. Retrieved from https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

02

OVERARCHING TRENDS

—

EXPRESSION

SECURITY

ECONOMY

The combination of detailed desk research and stakeholder input – via the survey and interviews – drew attention to several overarching trends that are central to any discussion of the cross-border legal challenges on the internet. These overarching 'meta-trends' are shaping topical trends (Chapter 3), and to a degree, they are setting the parameters within which the legal and technical approaches may be explored (Chapter 4).

First, some of the overarching trends relate to the changing technological landscape, which creates a need for 'future-proofing' any legal or technical approaches we embark on today. In this context, there is a clear trend of eroding borders between the online data-driven world and the physical world, and there is an equally clear trend of continuing migration to the cloud.

Second, some of the overarching meta-trends relate to the regulatory environment on the internet. While perhaps a rudimentary observation, there is a clear trend of recognition that legal regulation is necessary online – the question of whether to regulate or not is a 'dead issue'. A proliferation of initiatives signals that the cross-border legal challenges on the internet are being taken seriously, perhaps more so than ever before. Yet, the measures taken suffer from a lack of coordination and cooperation. This only compounds challenges arising from the trends of information overload and information access problems.

A third trend concerns serious attempts at re-thinking the role of territoriality for the regulation of the internet, and an emerging political will to do so. Indeed, there is increasing recognition, in some settings, that territoriality is largely irrelevant. Lawmakers are also displaying a greater appetite for extending laws online, often in an 'extraterritorial' manner that affects individuals, businesses and organizations overseas, or indeed other states; we may now be in an era of jurisdictional 'hyperregulation' (Chapter 2.2.2). The increasing geographic reach of national laws may be seen as a natural response, where national laws are the only tools to address transnational issues. Nevertheless, this trend is associated with issues, including enforcement difficulties, and there is some irony in that applying more laws transnationally will encourage more cooperation, because it is often necessary for enforcement.

Fourth, there is a set of overarching trends that relate to normative plurality, convergence and cross-fertilization. Blurring the distinction between illegal content, content that violates terms of service and content that is objectionable has only augmented the diversity of normative sources. One trend observed in this context is a harmonization via company norms; another is judicial cross-fertilization driven by replication and imitation that does not always properly account for scalability issues. In this context, the Internet & Jurisdiction Policy Network's stakeholders pointed to a trend of newer and smaller actors being bound by decisions from established and larger actors. This in turn may motivate the development of what may be termed 'global south impact assessments'.

A fifth trend pertains to the increased complexity around the role of internet intermediaries. In some instances, these intermediaries are self-proclaimed gatekeepers; in others, they are involuntary gatekeepers. Sometimes, they are simply scapegoats and 'easy' targets for litigation and content restriction orders.

2.1

A technological landscape in constant flux

There is a necessary and constant interplay between law and technology, as developments in one sphere typically impact the other.

The constant interplay between law and technology occurs both online and offline. In the past, such developments were typically slow, gradual and relatively sporadic. In the online environment, however, major technological developments are fast, dramatic and numerous. This puts significant stress on the law-making apparatus and demands a degree of future-proofing that goes far beyond what has historically been required. The preparedness for this task often appears limited in industrialized countries and is nearly absent in many developing countries.

2.1.1

The unification of online and physical worlds

One clear overarching trend is the fact that borders between the online data-driven world and the physical world are eroding and becoming less clear, or even meaningless. This is an ongoing process and not something new. People no longer 'go online' – we are constantly online. This has been the case for several years and it is in large part due to the uptake of smartphones.

In the Internet of Things era, however, the speed with which these borders erode is increasing dramatically, with effects for all aspects of society. As one interviewed expert noted, the big data-driven companies we know from the online environment are increasingly using their data-focused expertise to expand into traditional industries in the physical world (self-driving cars are one example, but this trend extends far beyond that). By the same token, traditionally offline companies are increasingly repositioning themselves as data-driven companies, but may still lack the capacity to fully engage with the breadth of cross-border jurisdictional issues because they are 'late to the party'. This raises several legal issues around competition, for example, and the abuse of dominant market positions. We are perhaps yet to see the full picture of how it will impact cross-border legal challenges online.

As several interviewed experts pointed out, technology in this context acts not only as an object of regulation, but as a regulatory force itself. Indeed, it has long been recognized that technology competes with law as a regulatory force, which in turn makes those in control of the technology into regulators.[36]

2.1.2

A continuing migration to the cloud

Put simply, cloud computing involves the on-demand provision of computing resources over the internet.[37] In this area, a distinction is routinely drawn between infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), but increasingly, also between government as a service (GaaS), monitoring as a service (MaaS) and security as a service (SECaaS).[38] All these forms of cloud computing have profound implications for cross-border legal challenges on the internet.

Whether intentionally or not, cloud computing typically creates connecting points to foreign jurisdictions in situations that may have previously been entirely domestic. Furthermore, cloud computing results in data being held by parties other than those who

---

36. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, 113, 506. Retrieved from https://cyber.harvard.edu/publications/1999/The_Law_of_the_Horse.

37. See further: Millard, C. (Ed.). (2013). *Cloud Computing Law*. Oxford, United Kingdom: Oxford University Press.

38. McGillivray, K. (2019). *Government cloud procurement: Contracts, data Protection, and the quest for compliance* (Doctoral dissertation). University of Oslo, Oslo, Norway, pp.55-56.

actually 'own' the data, which has consequences in relation to data privacy law, for example, and the ability of law enforcement to access content needed as evidence.

Cloud computing, with its often highly fluid data flows, may make it difficult or even impossible[39] to ascertain, in real time, where specific data is located. This, in turn, severely undermines the usefulness of data location as a jurisdictional connecting factor or focal point. As argued recently by a US court, when it is impossible to ascertain the location of data, it also becomes harder to argue that the sovereignty of a particular state was implicated when that data was accessed by a law enforcement agency: "Even if the interference with a foreign state's sovereignty is implicated, the fluid nature of Google's cloud technology makes it uncertain which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process."[40]

It is important, of course, to not confuse the question of *which* state's sovereignty is being interfered with, and the question of whether *any* state's sovereignty is being interfered with. The court's reasoning here may be accused of failing to recognize this distinction. Nevertheless, there is certainly some merit in the issue to which the court seeks to bring our attention.

While the study of cloud computing as a distinct regulatory or legal field seems to have declined, technological development is ongoing. Furthermore, states,[41] businesses,[42] and regions[43] are still developing ways in which they use cloud computing, and not all attempts at establishing cloud computing arrangements have been successful. One interviewed expert stressed that it is not only data that goes into the cloud. As massive amounts of software move into the cloud environment, ensuring control and security is a challenge, and security is not always built in from the start. Consequently, there is little doubt that cloud computing will continue to impact cross-border legal challenges on the internet as an overarching meta-trend.

2.2

Regulation: not if, but how and by whom

It is useful to distinguish between regulation *of* the internet, on the one hand, and regulation on the internet, on the other. It is primarily the latter that is in focus here.

2.2.1

To regulate or not is not the issue

During the 1990s, a debate raged about whether it was desirable to regulate cyberspace, and whether it was even possible to do so. This debate took place on several levels; in policy circles and in academia, and domestically and internationally among the comparatively limited number of states that were active online at that time. In the academic arena, key contributions to the English-language debate were made, not least, by several prominent North American scholars.[44]

Most famously, in the policy context, 1996 saw Barlow present his well-known *Declaration of the Independence of Cyberspace*, which captured the spirit of the time:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask

> "It is generally recognized that there is a need for legal regulation for many online activities."

39. In re Search Warrants Nos 16-960-M-01 and 16-1061-M to Google, para 7.

40. In re Search Warrants Nos 16-960-M-01 and 16-1061-M to Google, para 25.

41. Australian government. (2018). *Australia's tech future.* Retrieved from https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf.

42. Software One. *Managing and understanding on-premises and cloud spend.* Retrieved from https://www.softwareone.com/en/learn-and-inform/ebooks-and-whitepapers/survey-on-premises-and-cloud-spend.

43. See e.g., European Commission. *Digital single market: Cloud computing.* Retrieved from https://ec.europa.eu/digital-single-market/en/cloud.

44. Johnson, D.R. & Post, D.G. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48, 1367; Reidenberg, J.R. (1998). Lex Informatica. *Texas Law Review*, 76(3), 553; Geist, M. (2001). Is there a there there? Towards greater certainty for internet jurisdiction. *Berkeley Technology Law Journal*, 16, 1345; Menthe, D.C. (1998). Jurisdiction in cyberspace: A theory of international spaces. *Michigan Technology Law Review*, 4(1), 69; and Goldsmith, J.L. (1998). Against cyberanarchy. *University of Chicago Law Review*, 65(4), 1250.

you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. [...] You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. [...] Cyberspace does not lie within your borders. [...] Ours is a world that is both everywhere and nowhere, but it is not where bodies live. [...] Your legal concepts of property, expression, identity, movement, and context do not apply to us. [...] Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose."[45]

Today, some of these thoughts may seem to belong to a bygone era. Yet, other aspects are clearly still relevant – perhaps more as an explanation of the regulatory issues the ecosystem still faces today, rather than a manifesto. Sovereignty and enforcement remain complex and controversial issues. Cyberspace may be less 'borderless' now than it was then, but the clash between laws grounded in territoriality and a *prima facie* borderless, virtually global internet remains. Furthermore, some legal concepts are still difficult to transpose onto the online environment.

Nevertheless, questions of whether it is possible, and desirable, to regulate cyberspace are now 'dead issues'. It is generally recognized that there is a need for legal regulation for many online activities. For example, few would accept the idea of an online environment where laws against child abuse-materials do not apply. Consumers are less likely to engage in e-commerce if they are not afforded protection, and data privacy protection is at least as important online as it is offline. The fact that legal regulation plays an important role online is an important overarching meta-trend that affects every aspect of the topical trends (Chapter 3), and the legal and technical approaches (Chapter 4).

At any rate, the areas in relation to which the ecosystem relies on legal regulation are not necessarily static. As discussed in more detail below, while law is largely relied upon to create trust in online commercial transactions today, blockchain-based smart contracts may increasingly act as a competitor in some areas – even if the law remains an underlying facilitator of the trust created by smart contracts (Chapter 3.3.5.3).

Meanwhile, the applicability of law online is now firmly established. Scholars such as Ost, van de Kerchove[46] and Weitzenboeck[47] have emphasized that the pyramidal model of regulation – characterized by the centrality of the state as the regulator – has been severely undermined by developments in information technology, globalization, economic interdependence, human rights focus and the rise of transnational organizations. As summarized by Weitzenboeck, the resulting 'network regulation' or 'mesh regulation' that is argued to have replaced the pyramidal model of regulation sees:

"the state ceases to be the sole source of sovereignty (having to share this not just with super-state authorities but also with powerful private entities); the will of the legislator ceases to be received as dogma (it is accepted only subject to conditions, after a complex evaluation process both ahead and after the enactment of a law); the borders between fact and law at times become blurred; the different powers of the state interact (judges become co-authors of the law and the sub-delegation of normative power which, in principle was prohibited, multiplies); the juridical systems (and, more broadly, the normative systems) become entangled; knowledge of the law which traditionally proclaimed its methodological purity (mono-disciplinary) now leans towards an interdisciplinary mode and is more the result of a learning process than a priori axioms. Moreover, justice, which in the pyramidal model was reduced to the hierarchies of values fixed in the law, is today understood in terms of the balance of interests and the equilibration of values which are both different and variable."[48]

Self-regulation

Self-regulation has played a major role in the development of the internet and can occur on a variety of levels, ranging from infrastructure governance to peer-driven content moderation within a specific online forum. The domain name system is often cited as a prime example of successful self-regulation. As another example, one interviewed expert cited the self-regulation of counter-terrorism measures on the internet, as opposed to externally imposed rules. More broadly, another interviewed expert stressed the need for international agreement on standards of jurisdiction on the internet, because while companies should be encouraged to self-regulate, governments need to take responsibility, as well.

It is possible, however, that the wind is changing on self-regulation of companies (even in the US). Indeed, ICANN today could be seen as more of a hybrid organization, as governments play an increased role in its regulation.

---

45. Barlow, J.P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/cyberspace-independence.

46. Ost. F, & van de Kerchove. M. (2002). De la pyramide au réseau? Pour une théorie dialectique du droit, *Facultés universitaires Saint-Louis Bruxelles*.

47. Weitzenboeck. E, (2014). Hybrid net: the regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology*, 22(1), 49.

48. Weitzenboeck. E, (2014). Hybrid net: the regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology*, 22(1) 49, 68.

Whether this paradigm shift has been completed, is merely under way, or indeed is overstated, may be a topic open for discussion. However, it is undeniably the case that we are witnessing signs of these trends, and they are both driven by the online environment and fundamentally impacting the cross-border internet issues of concern in this Report.

Further, while we have moved far from Barlow's Declaration, the era of so-called self-regulation is by no means over. And indeed, there are several regulatory types of prominence in the online landscape, including:

1. private law regulation;
2. public law regulation;
3. private-public arrangements;
4. self-regulation; and
5. technical code or lex informatica.[49]

The first four, but normally not the fifth, of these regulatory types may be country-specific and vary considerably from country to country. This further complicates the regulatory landscape.

Here we may pause to consider how regulatory initiatives, falling into these different regulatory types, from different parts of the world interact. At least five options may be identified. Different regulatory initiatives may:

1. result in fundamental clashes;
2. result in minor clashes;
3. co-exist without interaction;
4. be interrelated; or
5. be interdependent.

Ultimately, regardless of regulatory type, regulating the internet requires a steady hand and a dispassionate mind. History has already proven that both inaction and over-action may be harmful for this sensitive and indeed fragile environment.

2.2.2

Proliferation of initiatives

A plethora of new initiatives from public and private actors around the world have been announced or adopted to address the issues at stake. These include new national laws, guidelines, Opinions, codes of conduct, model laws, multilateral agreements conventions, declarations, and company policies. Many of these initiatives are discussed in Chapter 3 that outlines key topical trends, and in Chapter 4 that analyzes a range of legal and technical approaches.

In this context, it is useful to pause to consider the hardening of so-called 'soft law' that is increasingly apparent[50]. Soft law taking a position on the proper interpretation of complex laws, such as the opinions and guidelines issued by many designated authorities or other bodies, frequently assumes a role virtually indistinguishable from hard law, such as legislation and case law. This is not only occurring in the online environment, but it can perhaps be said that it is particularly prevalent in internet regulation.

In any case, the intensive developments on cross-border legal challenges online signal that these issues are now taken seriously, which is certainly important. Yet, uncoordinated patching actions, taken in a reactive mode under the pressure of urgency, create a legal arms race with potentially detrimental impacts – an arms race involving the active deployment of measures rather than simply a stockpiling of potential measures. Ensuring that the multiplication of different regimes does not create additional tensions, or even conflicts, is a major challenge.

The degree to which states seek to apply their laws to internet activities has not been static over the years. In fact, it is possible to identify a pattern of pendulum swings between what may be described as 'jurisdictional under-regulation' on one side, and 'jurisdictional over-regulation' on the other.[51]

Today, the regulatory environment is clearly swinging toward jurisdictional over-regulation. Indeed, the appetite with which states are now seeking to extend their jurisdiction and apply their laws to internet activities is unprecedented. Thus, one may speak of this as an era of jurisdictional 'hyper regulation' characterized by the following conditions:

1. the complexity of a party's contextual legal system (i.e., the combination of all laws that purport to apply to that party in a given matter – see further Chapter 2.2.6) amounts to an insurmountable obstacle to legal compliance; and
2. the risk of legal enforcement of (at least parts of) the laws that make up the contextual legal system is more than a theoretical possibility.

One interviewed expert emphasized that governments are now seeking to control the online environment, which results in the creation of more laws, as their typical response is to introduce new laws rather than apply existing laws to confront the challenges.

A related trend is the fast pace at which political agendas and policy focuses change. For example, various online issues that gained limited

49. Weitzenboeck. E, (2014). Hybrid net: the regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology*, 22(1), 49.

50. See also: Weber, R. H. (2012). Overcoming the hard law/soft law dichotomy in times of (financial) crisis. *Journal of Governance and Regulation*, 1(1), 8-14.

51. See further: Svantesson, D. (2017). *Solving the internet jurisdiction puzzle.* Oxford, United Kingdom: Oxford University Press, 91-112.

attention just some years ago, such as online bullying, the spread of hate speech and non-consensual distribution of sexually explicit content, are now widely recognized as problems. The constant shifting of priorities and attention from one topic to another, often spurred by the news media, creates a sense of urgency that leaves governments with insufficient time to decide on, or coordinate, approaches.

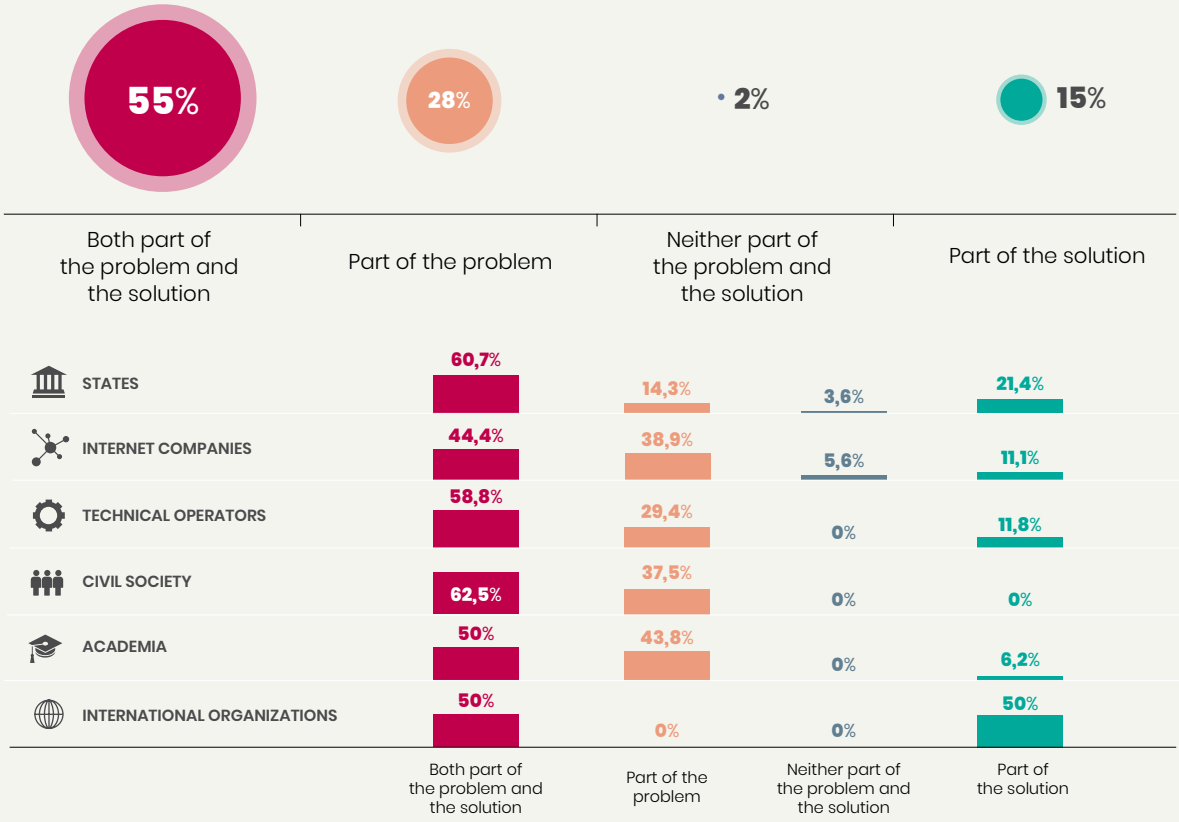
2.2.3

An increasing appetite to regulate cyberspace

Some interviewed experts noted that although governments in the past largely took the view that internet regulation was difficult or impossible, the political will to regulate the internet is now stronger than ever. Indeed, tech industry leaders are too increasingly calling for further regulation.[52] Just over half of surveyed experts indicated that they see this development as both part of the problem and part of the solution. In more detail, 55% indicated that the increase in the enforcement of national laws in cases involving servers, users or companies located in other countries is both part of the problem and part of the solution. 28% saw it as just part of the

INFOGRAPHIC 10

Increased regulation of cyberspace: problem or solution?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

52. See e.g. Internet & Jurisdiction Policy Network. (2019, March). Facebook calls for increased regulation pertaining to harmful content, elections, privacy and data portability. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTktMDMifQ==.

problem, while 15% saw it as just part of the solution. 2% saw the increase in the enforcement of national laws in cases involving servers, users or companies located in other countries as being neither part of the problem nor part of the solution.

In their comments, surveyed experts expressed concerns around the increased enforcement of national laws in cases involving servers, users or companies located in other countries. In particular, surveyed experts pointed to concerns about arbitrariness, uncertainty, unintended consequences, inappropriate impacts, and a tension between state priorities and a global vision. Others noted that while adherence to treaties would be ideal, in its absence, extraterritorial national laws – if properly implemented – are a sensible interim solution. Some also argued that unilateral attempts highlight weaknesses in existing regimes, and as such, work as an inevitable catalyst for long-term change.

There were clear sectoral differences on this survey question, with stakeholders from the government sector and international organizations being considerably more positive about this development.

2.2.4

Information overload and accessibility

To move forward on the cross-border legal challenges on the internet in the most successful way possible, all stakeholders must have access to relevant information. Indeed, this is one of the reasons for this Report. Yet, both the feedback provided by surveyed and interviewed experts, and indeed the very writing process of the Report have showcased the present obstacles preventing the level of access required for informed policy development.

One surveyed expert stressed that the translation of the judicial order is a major issue, and suggested that perhaps a language should be chosen as an official one just like in diplomatic relations. Some interviewed experts pointed to the strong dominance of the English language as a current problem in the context of accessing information, noting that the cost of translations is a limiting factor. However, it was also noted that this current barrier is likely to decline, as younger generations in many countries have high levels of English proficiency. One interviewed expert made the important observation that materials only being available in a foreign language forces reliance on brief secondary sources, which often lack nuance and are written for a generalist audience. This reality plagues all stakeholder groups and is also a legitimate concern in relation to some of the materials relied upon for this Report.

One surveyed expert stated that information was accessed mainly on a regional scale. Another noted that, although there is substantial information available about decisions in the US and Europe, there is not much information about decisions and developments in other states – including their rationale, their laws and the interpretation of those laws. This could be seen as a call for states around the world to do more to provide and promote free online access to their laws and court decisions, preferably with key developments accessible in multiple languages.

This observation is also of interest in relation to the widespread lack of issues and examples from other regions (outside the EU and US) in discussions of cross-border legal challenges on the internet – a problem strongly emphasized by numerous interviewed and surveyed experts. Surveyed and interviewed experts noted that much is being done to ensure regional diversity in the discussions, including greater representation from developing countries. Yet one may reasonably assume that part of the problem stems from EU/US developments becoming the common denominator in the discussions, partly due to their accessibility. As a result, these developments garner greater attention at the expense of examples from other regions, even when those regions are represented in discussions.

"To move forward on the cross-border legal challenges on the internet in the most successful way possible, all stakeholders must have access to relevant information."

Variance in access to materials from different regions

Numerous surveyed and interviewed experts pointed to the **I&J Retrospect Database** of the Internet & Jurisdiction Policy Network as a leading source of information on the relevant actors and initiatives, the details of relevant laws and their application, as well as the relevant court decisions in the topic of cross-border legal challenges on the internet.
However, the wide variance in access to materials from different regions is also reflected in the Internet & Jurisdiction Policy Network's Retrospect Database.[53] For example, an examination of the reported cases during the year of 2018 – 240 in total – reveal the following statistics:

- 95 of these deal exclusively with Europe, and another 12 involve Europe plus at least one other jurisdiction;
- 28 cases deal exclusively with North America, and another 12 involve North America plus at least one other jurisdiction;
- 19 cases are geographically neutral;
- 17 cases deal exclusively with Asia (apart from China, India and Russia), and another 1 involves Asia (apart from China, India and Russia) plus at least one other jurisdiction;
- 14 cases deal exclusively with Russia, and another 1 involves Russia plus at least one other jurisdiction;
- 10 cases deal exclusively with India, and another 1 involves India plus at least one other jurisdiction;
- 9 cases deal exclusively with South America, and another 2 involve South America plus at least one other jurisdiction;
- 8 cases deal exclusively with Australia/New Zealand, and another 2 involve Australia/New Zealand plus at least one other jurisdiction;
- 9 cases deal exclusively with China;
- 9 cases deal exclusively with Africa; and
- 7 cases deal exclusively with the Middle East, and another 1 involves the Middle East plus at least one other jurisdiction.

While the Internet & Jurisdiction Policy Network's Retrospect database is clearly intended to capture information from around the world, the dominance of European materials is nevertheless overwhelming. This highlights the need for more and better information sharing, and points to the usefulness of future regional reports.

In this context, it is worth emphasizing the point that information sharing equals impact. For example, if a person from South America meets someone from Asia and neither knows much about the other's laws and approaches, but both have a basic understanding of European and North American approaches, they are perhaps likely to base their discussion on the common knowledge they share. This results in a 'disproportionate' influence of European and North American law, which is a key issue for both capacity building and inclusiveness. Here we may usefully reconnect with the language issue discussed above. An increasing English language proficiency may eradicate current language barriers on the receiver side; i.e. access to English language materials in non-English language states may not be much of an issue. However, language barriers will remain a considerable hurdle on the provider side. The likely result is that people from non-English states are becoming skilled at accessing/consuming English language information, but still lack effective means for making their non-English language laws etc accessible to people that do not speak their language. Thus, the increase in English proficiency may work against the influence of non-English speaking countries.

The need for capacity building was a recurring theme in comments from surveyed and interviewed experts, and it is relevant in this context, as well. For example, one interviewed expert commented on the importance of developing a new way to educate policy makers, regulators and others, so that the discussion remains robust in terms of legal tradition, but in a way that can be readily understood to prevent these stakeholders from 'switching off'. Interviewed experts from the tech sector made similar comments on capacity building, with some stressing the need for legislators and law enforcement to understand the technology and terminology.

---

53. Internet & Jurisdiction Policy Network. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect.

2.2.5

Every problem has a solution, but every solution has a problem

One may argue that judicial and legislative creativity has declined over recent years. Yet, solutions have been, and are being, advanced to address the complications regarding the establishment of a court's personal jurisdiction over a defendant in another territory. Many will recall, for example, the 'sliding scale' test articulated by US courts in the mid-1990s, which sought to organize websites by reference to their 'interactivity'.[54] And in the famous High Court of Australia case in 2002 between US publishing company Dow Jones and Victorian businessman Gutnick – which marked the first time that the highest court of any state considered the matter of jurisdiction over cross-border internet defamation – Justice Kirby determined that the solution was found in the doctrine of *forum non conveniens*.[55]

These solutions, like many others, have not stood the test of time. But the judicial self-restraint that Justice Kirby anticipated in the form of *forum non conveniens* is still frequently cited as a potential solution, even though court attitudes toward jurisdiction appear to be moving away from self-restraint.[56]

Therefore, few proposed solutions are truly 'new', and focusing on whether they are or not is arguably not the most fruitful approach. More importantly, though, is how well a given solution addresses the concerns at hand.

The reality is that jurisdictional issues both online and offline are complex, and considering the attempts at finding solutions so far, it seems clear that perfect solutions are improbable; indeed, the search for perfection can become an obstacle to progress. And given that the world is increasingly characterized by complexity, arriving at an all-encompassing international treaty to solve the myriad cross-border legal challenges online is highly unlikely in the foreseeable, and even distant, future.

> "Perfect solutions are improbable [...] the search for perfection can become an obstacle to progress"

Rather than waiting for the problems to go away, or to be resolved through an unlikely international treaty, stakeholders need to continue working on many different fronts and ensure that their work is as coordinated as possible. Such work should also be grounded in solid conceptual frameworks – a component that is typically provided by academic research.

Yet, despite the central role that the internet plays in modern society, and despite its increasing prominence in policy discussions, cross-border legal challenges on the internet are still treated as fringe issues in legal academic literature – not least within the fields of public and private international law. This is untenable. Cross-border internet-related legal issues are central matters in society today, and this must be reflected in public and private international law discussions.

Regrettably, it appears that the legal issues of internet jurisdiction are receiving less attention in legal academic literature.

Cross-border legal challenges arise within virtually all areas of substantive law and are often approached and debated within the context of each area. For example, these challenges may be discussed in the context of reforming intellectual property law, defamation law, cybercrime or taxation.

It is also important to recognize that one can approach the cross-border legal challenges on the internet as a topic in its own right, and not merely as a component of different substantive law areas. Doing so reveals the extent to which identical or similar jurisdictional challenges arise in different settings, allowing solutions and approaches from one context to be transposed to another. Further 'meta-level' work of this kind is needed in this area.

---

54. Zippo Manufacturing Company v Zippo Dot Com, Inc 952 F.Supp 1119 (WD Pa 1997).

55. Dow Jones & Company Inc v Gutnick (2002) 210 CLR 575. For a recent discussion of the doctrine of *forum non conveniens* in relation to the internet, see: Haaretz.com v. Goldhar, 2018 SCC 28, 2018 2 S.C.R. 3.

56. See, however, Advocate General Szpunar's call for courts to adopt an approach of 'self-limitation' (Opinion in Case C-18/18, para 100), as well as the CJEU's emphasis on the diversity of laws (Case C-507/17).

Jurisdictional issues represent a decreasing proportion of academic work

Year	1994-1998	1999-2003	2004-2008	2009-2013	2014-2018
Number of journal articles addressing the legal issues of internet jurisdiction[57]	841	1,997	1,451	1,501	1,281
Number of journal articles addressing the internet[58]	13,762	31,646	34,680	39,392	37,981
Percentage of journal articles addressing the legal issues of internet jurisdiction out of total number of journal articles addressing the internet	6.1%	6.3%	4.2%	3.8%	3.4%

2.2.6

Legal uncertainty increases

The activities of both natural persons (individuals) and legal persons (companies and other organizations) are regulated by law. In the offline environment, it is typically quite easy to identify the applicable law. For example, a person driving a car on roads in Germany is subject to German traffic rules. Identifying the applicable law(s) online is often more complicated.

When sending an email from Argentina to Japan, for example, a person may be subject to both the laws of Argentina and those of Japan. However, when the same person in Argentina posts a defamatory comment about a person in Finland to a social media site, she may be subject to not only the laws of Argentina and Finland, but the laws of all the countries in which she has contacts in her social media network – and perhaps any law specified in her agreement with the social media platform. As this example shows, it is important to bear in mind that applicable laws are determined by the activities we undertake.

To understand the complications that arise, it is useful to think of the laws that apply to a person in a given situation as a 'contextual legal system' – that is, a system of legal rules from different states that all apply to the activity undertaken by that person. It is then clear that, in the example involving an email sent from Argentina

57. This study is based on a text search for journal articles either containing at least one sentence with both the term "internet" and the term "jurisdiction", or at least one sentence with both the term "Cyberspace" and the term "jurisdiction" (i.e. (Cyberspace /s jurisdiction) OR (Internet /s jurisdiction)). The searches were carried out on 7 January 2019 on the Law Journal Library of HeinOnline. The search was limited to the following categories: "Articles", "Comments", "Notes" and "Editorials", and included "external articles (articles outside of HeinOnline)" as well as "periodical results from other HeinOnline Collections". This approach admittedly has its limitations. Nevertheless, the result is indicative of the development in academic law journal articles, comments, notes and editorials addressing the topic of internet jurisdiction.

58. Result produced via the following search: (Cyberspace OR Internet). The searches were carried out on 7 January 2019 on the Law Journal Library of HeinOnline. The search was limited to the following categories: "Articles", "Comments", "Notes" and "Editorials", and included "external articles (articles outside of HeinOnline)" as well as "periodical results from other HeinOnline Collections".

to Japan, the contextual legal system is less complex (because it consists of the legal rules of two states) than that of the latter example involving a defamatory social media posting.

A serious problem online is that people are often unable to predict all the states' laws that form part of their contextual legal system for any given activity. Even when persons can ascertain which states' laws apply to them, it is not always easy to access all those laws. Indeed, even where access can be ensured, language issues may preclude a full understanding of those laws. In addition, the legal rules of a domestic legal system are typically structured to avoid situations where one legal rule demands something that another legal rule prohibits. However, where a contextual legal system consists of legal rules from different states – as is typically the case in relation to online activities – no such coordination can be presumed. As a result, it is not uncommon online for one legal rule, within a relevant contextual legal system, to require something that another legal rule within the same system prohibits. This lack of legal harmonization, while natural considering how the world is organized, is a major hurdle, as it creates an environment in which ensuring legal compliance is difficult, or even impossible.

This poses obvious practical challenges. On a deeper level, it also undermines the legitimacy of at least one fundamental legal principle: the principle that ignorance of the law excuses not ('*Ignorantia juris non excusat*'), which is a cornerstone of any functioning legal system. If one acknowledges that the regulatory environment online makes it frequently impossible to be informed of one's legal obligations, it is difficult to maintain that ignorance of the law is no excuse. For now, the general impossibility of knowing all the laws that purport to apply, and the fact that ignorance of the law is typically no excuse, seem irreconcilable, affecting both the topical trends (Chapter 3), and the legal and technical approaches (Chapter 4).

Furthermore, in any situation involving clashing norms, we should not restrict ourselves to something as crude as assessing whether a given country's laws apply to the situation, because not all laws of a country are relevant in any given situation.

Imagine that legal person Y from state A enters into a purchase contract with natural person Z from state B. If state B wants to apply its consumer protection laws to the situation, those laws of state B may have a substantial connection to the matter and state B may have a legitimate interest in applying those consumer protection laws. However, if state B, based on the same set of facts, wants to apply its corporate governance laws to Y, the connection is weaker and the interest in doing so is less legitimate. To take this example to the extreme, imagine that based on the mentioned scenario, state B wants to apply its marriage laws to all employees of legal person Y; then both the connection and the interest is non-existent.

Thus, any assessment of whether state B's laws shall apply hinges on what norms that state seeks to apply. It is the applicability of individual norms of a certain state, rather than all its laws in their entirety, that should be in focus. This increased granularity ought to be reflected in private international law rules, especially where they are affecting the online environment.

"A serious problem online is that people are often unable to predict all the states' laws that form part of their contextual legal system for any given activity. Even when a person can ascertain which states' laws apply to them, it is not always easy to access all those laws."

2.3

Rethinking the role of territoriality

In relation to the matter of jurisdiction, territoriality is essentially meant to fulfil two functions. The first is to provide a criterion for when a state can claim jurisdiction. Online, however, it is particularly easy to find territorial anchor-points for jurisdictional claims. The second function of territoriality is to act as a 'stop sign' that provides a warning when one enters the exclusive domain of another state. Here again, though, territoriality fails online.

It is simply unrealistic to think that a state will be part of the global community and still enjoy traditional exclusiveness, in the Westphalian sense.

In fact, it seems increasingly obvious that drawing a distinction between territorial and extraterritorial jurisdictional claims is misguided. This is because:

1. There is no (international) agreement on when a claim of jurisdiction is extraterritorial (which, assuming that extraterritorial is the opposite of territorial, logically precludes any agreement on when a claim of jurisdiction is territorial); and
2. Some 'extraterritorial' claims of jurisdiction are clearly supported in international law, as is the case, for example, under the nationality principle. In fact, exceptions to a strict adherence to territoriality are now so numerous that territoriality can no longer be seen as the jurisprudential foundation for jurisdiction.

Even where a jurisdictional rule is drafted in terms of territorial criteria, its true underlying aim is to establish whether the state making the jurisdictional claim has a sufficiently strong connection to the matter to create a legitimate interest in claiming jurisdiction; a territorial criterion is merely a proxy for this underlying aim. For example, while Article 3 of the GDPR purports to delineate the GDPR's scope of application in a spatial sense, it actually does so in a manner that is both territoriality-dependent and territoriality-independent. In the end, the binary nature of the distinction between territorial vs. extraterritorial fails to account for the true nature of the reality with which we work.

To speak of extraterritoriality is akin to describing cars as 'horseless carriages' – both descriptions are founded in a mistaken notion of what is 'normal'. Although the term 'extraterritoriality' is still widely used for the sake of convenience, we must be aware that extraterritoriality, as a concept, has been discredited.[59]

It is well established and beyond intelligent dispute that international law's focus on territoriality is a bad fit with the fluidity of the online environment, which is characterized by constant and substantial cross-border interaction. Yet, until recently, little had been done, and even less achieved, in the pursuit of disentangling internet jurisdiction from territoriality.

In policy documents and academic writings, the most commonly cited source for a territoriality focus is the classic *Lotus case*[60], which was decided by the then-Permanent Court of International Justice in 1927. This case involved a collision between two steamships.

While principles articulated in one setting may legitimately be applied to cases in other settings, cases concerning colliding steamships clearly differ from those in the context of internet jurisdiction. And while legal principles should not be abandoned merely because they are old, nor should they be beyond reappraisal just because they are old. Given that general legal methods call for treating different cases differently, there seems to be little point in grounding our thinking on internet jurisdiction in the *Lotus* decision. In fact, the majority opinion in *Lotus* emphasized the need to focus on "precedents offering a close analogy to the case under consideration; for it is only from precedents of this nature that the existence of a general principle applicable to the particular case may appear."[61]

> "Rather than conceding that the absence of relevant case law means that this is an unsettled area of law, there has been a tendency to inappropriately overemphasize the *Lotus* decision."

59. See further: Ryngaert, C. (2015). *Jurisdiction in International Law 2nd edn*. Oxford, United Kingdom: Oxford University Press, p. 8.
60. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10, p. 21.
61. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10, p. 21.

Perhaps the real reason that the *Lotus* decision still receives so much attention is the fact that there are so few other international decisions on this topic. Rather than conceding that the absence of relevant case law means that this is an unsettled area of law, there has been a tendency to inappropriately overemphasize the *Lotus* decision.

Moreover, the *Lotus* judgment is not a particularly solid foundation for the territoriality principle, because it contains contradictions and lacks clarity in some areas. It is also a decision in which no less than half of the members of the court expressed a dissenting opinion, and there is not even any agreement as to what type of jurisdiction – prescriptive, judicial or enforcement – the *Lotus* case involved.

As the role of strict territoriality declines in the context of jurisdiction, something else must take its place as the jurisprudential core of jurisdictional claims. In the context of law enforcement access to digital evidence there are, at least, signs of an emerging consensus[62] to focus on whether the state claiming jurisdiction has a legitimate interest and a substantial connection to the matter at hand, combined with an assessment of the consideration of other interests.[63] Discussions regarding the cross-border legal issues associated with law enforcement access to digital evidence are relatively advanced, and as one interviewed expert noted, this field is a major driver in cross-border legal issues. Therefore, reliance on this three-factor framework may spread, as it can also be applied in other settings in which standards need to be imposed on claims of jurisdiction.[64]

Focusing on whether the state claiming jurisdiction has a legitimate interest and a substantial connection to the matter at hand, combined with an assessment of the consideration of other interests, has the advantage of incorporating a wide range of complex international law concepts, while also being easily understandable. This user-friendliness makes it an effective tool to overcome some of the 'artificial regulatory challenges' associated with cross-border legal issues on the internet. It further benefits from being relevant for both matters that traditionally fall within public international law and those that traditionally fall within private international law (or conflict of laws).

2.3.1

An increasing geographic reach of national laws

When jurisdictional rules are broad in scope, they risk capturing conduct with which there is an insufficient degree of contact to justify a state's jurisdictional claim. This may lead to jurisdiction being exercised over parties that lack adequate notice. At the same time, when jurisdictional rules are narrow in scope, they risk leaving victims without judicial redress. Striking the right balance is no easy task, and focusing on distinctions between territoriality and extraterritoriality frequently leads to both of these problems.

Many states make broad claims of jurisdiction over internet activities – claims that they cannot possibly back up with effective enforcement. While common, such 'jurisdictional trawling' is often a destructive regulatory approach, especially when it leads to arbitrary enforcement, which, as interviewed experts emphasized, is a poor fit with the rule of law.

In addition, as states compete to have their laws respected, many are increasing the potential fines for those who fail to comply. This is problematic in instances where compliance with one state's law necessitates the violation of another state's law.

The aforementioned 'jurisdictional trawling' and high potential fines are merely two examples of states flexing their muscles in relation to the internet. Comparing the issue of jurisdiction online and offline, arguably the biggest difference is that for online jurisdiction, there is a greater need to link the question of whether a claim of jurisdiction is appropriate with the question of over what jurisdiction is asserted. Put differently, it is harder in the online context to determine which aspects of a legal or natural person's activity are captured by a claim of jurisdiction and which are not. This is a topic that has so far gained little attention, and there is a clear need for more sophisticated tools to ensure that claims of jurisdiction are not broader than necessary to accomplish lawmakers' goals.[65]

Yet, perhaps the biggest challenge relates to trying to change attitudes. of-

---

62. Internet & Jurisdiction Policy Network. *Data & jurisdiction program: Operational approaches.* Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf.

63. These 'other interests' may include the interests of individuals, see e.g., the work of Ireland-Piper regarding whether the 'abuse of rights' doctrine might be helpful in seeking to maintain an appropriate balance between the rights of states and of individuals (Ireland-Piper, D. (2017). *Accountability in extraterritoriality*. Cheltenham, England: Edward Elgar).

64. See further: United Nations Special Rapporteur on the Right to Privacy Task Force on Health Data. (2019). *Draft recommendation on the protection and use of health-related data.* Retrieved from https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf, and Svantesson, D. (2017). *Solving the internet jurisdiction puzzle*. Oxford, United Kingdom: Oxford University Press, pp. 57-90.

ten, the aim of the rules of jurisdiction is understood to be to merely further the domestic policy objectives of relevant substantive laws. For example, if defamation law aims to protect the reputation of individuals, the aim of relevant jurisdictional rules is perceived to be to make the substantive defamation law as widely enforceable as possible by extending the claim of jurisdiction globally. But this is too simplistic. The underlying role of rules of jurisdiction must always be to seek the effective enforcement of the relevant substantive law, while at the same time minimizing, or even avoiding, the risk of international tension and conflict, and without imposing unreasonable burdens on those subjected to the regulation.

2.3.2

Challenges of enforceability

It is easy to understand why states want their laws to be respected online in the same way they are respected offline. Indeed, as the world is structured today, each state may be understood to have the right to dictate what is available online in that state. At the same time, despite the obvious legitimacy of their ambition for online and offline legal parity, there are several other considerations that must be part of the equation.

First, merely claiming that a state's laws apply worldwide online does not make it so. International law imposes some restrictions – albeit vague ones – on when a state can claim that its laws apply. Furthermore, a state's ability to enforce its laws is often more limited than the claims it makes regarding the reach of its laws.

Second, as states make broader jurisdictional claims, they may become increasingly dependent on the cooperation of other states for the enforcement of those claims. Therefore, although broader claims of jurisdiction may lead to obvious clashes in some cases, they may also encourage greater cooperation and coordination among states.

Any potential positive impact of broader jurisdictional claims may be lost when states are content to limit themselves to what may be termed 'domestic enforcement of extraterritorial claims'. Rather than relying on enforcement through the cooperation of foreign states, states, in this scenario may impose 'market destroying measures' on the foreign party, such as restricting that party's access to users in the country in question.[66] Such exercises of 'market sovereignty' are seemingly increasing in frequency.

Third, where a state makes the claim that its laws apply to certain online activities, it needs to be prepared to accept equally broad claims from other states.

Fourth, jurisdictional hyperregulation (Chapter 2.2.2) imposes a significant cost of compliance on all natural and legal persons who seek to abide by the applicable laws. Fifth, there is a risk that natural and legal persons who seek to abide by all applicable laws adhere to the strictest standards, under the logic that compliance with the strictest standards ensures compliance with all relevant laws. Such an approach is ill-advised as there is not one state that has the strictest laws on every topic. Thus, to know which law is the strictest on any given topic, one needs to know all the laws of all the states in the world. Further, it may spark a 'race to the bottom' with the risk of irreversible consequences for diversity online.

Taken together, these considerations suggest that the legitimate aim of having state laws respected online in the same way as offline must be pursued in a careful and intelligent manner. In our current era of jurisdictional hyperregulation (Chapter 2.2.2), there is a clear meta-trend of states making overly broad and diction where more limited, intelligent and nuanced claims of jurisdiction would:

1. be easier to defend both morally and under international law;
2. be easier to enforce;
3. impose lower compliance costs; and
4. be less likely to encourage overly broad claims of jurisdiction by other states.

"As states make broader jurisdictional claims, they may become increasingly dependent on the cooperation of other states for the enforcement of those claims. Therefore, although broader claims of jurisdiction may lead to obvious clashes in some cases, they may also encourage greater cooperation and coordination among states."

65. For examples of attempts at constructing such tools, see e.g., Svantesson, D. (2013). A 'layered approach' to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3(4), 278-286; and Svantesson, D. (2017). *Solving the internet jurisdiction puzzle*. Oxford, United Kingdom: Oxford University Press, pp. 171-189 outlining a framework for 'scope of jurisdiction'.

66. See further: Svantesson, D. (2016). *Private international law and the internet* (3rd ed.). Alphen aan den Rijn, The Netherlands: Kluwer Law International, pp. 11-12.

2.3.3

When territoriality is irrelevant

Given the above, it is only natural that we have seen a slow but steady decline in the focus on territoriality for jurisdictional purposes. As discussed in Chapter 3.2.2.3, some recent examples of this include the 2018 US CLOUD Act; the EU's *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*[67]; and the EU's *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.*[68] The ongoing work on the Council of Europe's 2nd Additional Protocol amending the Budapest Convention is another example. Further, Article 3(1) of the EU's GDPR specifically emphasizes that the location of data processing is irrelevant (Chapter 3.1.6.1). With these instruments, the EU and US are shifting their focus away from the location of the data in question, and from territoriality more broadly.

It has also been noted that soft law is "a regulatory model which develops and establishes rules independently of the principle of territoriality".[69] This is significant since, as noted above, soft law is particularly prevalent in internet regulation.

The shift away from blind adherence to territoriality as the foundation of jurisdiction must be understood in light of the fact that territoriality-based thinking encourages data localization (Chapter 4.2.7), and fragmentation more broadly. Furthermore, as noted, territoriality, as a concept, suffers from several weaknesses, especially when applied in online contexts where determining the location of a specific activity necessitates entering the quagmire of legal fictions.

> "Jurisdiction, as a jurisprudential concept, is not rooted in territoriality."

At the same time, it should be noted that difficulties in applying the concept of territoriality are by no means limited to the online environment. Such difficulties are also common offline, particularly in fields such as human rights law, aviation law and anti-competition law. It is time to recognize that what are normally discussed as 'exceptions' to the territoriality principle are too numerous, and too important, to be seen as mere exceptions. These exceptions must instead be recognized for what they really are: indicators that jurisdiction, as a jurisprudential concept, is not rooted in territoriality.

2.4

Normative plurality, convergence and cross-fertilization

It is a well-established fact that law is not the only factor affecting conduct online.[70] Indeed, law does not always have the greatest effect on conduct online. This has profound implications.

2.4.1

Blurring of categories

Interviewed experts noted that there is sometimes a fine line between legitimate political speech on the one hand, and hate speech or defamatory content on the other. Some measures aimed at removing the latter risk suppressing the former. One interviewed expert also observed that there is no broad agreement on norms, behaviors and types of content that are universally acceptable. The international differences are great; content may be

67. COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.
68. COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.
69. Weber, R. H. (2012). Overcoming the hard law/soft law dichotomy in times of (financial) crisis. *Journal of Governance and Regulation*. 1(1), 8-14, 12.
70. See e.g.: Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, 113, 506. Retrieved from https://cyber.harvard.edu/publications/1999/The_Law_of_the_Horse.

classified as hate speech in one jurisdiction, for example, while it may be classified as acceptable in another. Interviewed experts underscored this point by drawing a comparison between how the US and Germany treat hate speech.

In a 2012 Report, the UN Special Rapporteur on Freedom of Expression pointed to three different types of expression: (1) expression that constitutes an offense under international law and can be prosecuted criminally; (2) expression that is not criminally punishable but may justify a restriction and a civil suit; and (3) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others. This remains a useful categorization, and as noted by the Special Rapporteur, these categories of expression pose different issues that call for different legal and policy responses.[71]

If these categories are not taken into consideration, distinctions between illegal content, content that is contrary to terms of service and objectionable content may become blurred. Such blurring must be avoided, especially given that, as affirmed by the UN Human Rights Committee, Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR) protects the expression of opinions and ideas, even if some individuals may see them as deeply offensive.[72]

Drawing upon the aforementioned work, it may be possible to point to the following six types of expression:

The six types of expression:

1. Expression that constitutes an offense under international law and can be prosecuted criminally
2. Expression that constitutes an offense under national law and can be prosecuted criminally
3. Expression that is not criminally punishable but may be actionable under civil law
4. Expression that is not against applicable law, but violates relevant terms of service or other soft law
5. Expression that is neither against applicable law, nor relevant terms of service or other soft law, but seen by some as objectionable[73]
6. Expression that is entirely uncontroversial

It may be tempting to view this structure as a form of ranking. Doing so, however, involves at least one inappropriate simplification: not all laws are made equal. It is often argued that laws should trump terms of service, because laws are the result of an established democratic process, whereas the terms of service are unilaterally imposed by profit-driven corporations. This reasoning does not lack merit, but if the superior position of laws is founded upon their democratic pedigree, what about laws that are not based on democratic processes? What is, for example, the proper relationship between terms of service and dictatorial laws aimed at suppressing democratic movements? This is an important topic that deserves further study.

---

71. Annual report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to the General Assembly. (2012). A/67/357, para. 2. Retrieved from https://undocs.org/en/A/67/357.

72. United Nations, Human Rights Committee. (2011, September 12). *General Comment No. 34 on Article 19: Freedoms of opinion and expression.* CCPR/C/GC/34, para 11. Retrieved from https://undocs.org/en/CCPR/C/GC/34.

73. This category is broad and covers e.g. offensive content as well as misinformation and content that can increase the risk that its audience will condone or commit violence against others.

2.4.2

Harmonization via company norms

Another notable overarching trend is the comparatively high degree of transnational harmonization through company norms, versus the fractured country-based norm setting and decision making. There is a considerable degree of harmonization across the norms (e.g., terms of use, terms of service) implemented by the major (US-based) internet platforms. This may be explained, in part, by the fact that these platforms are subject to the same legal requirements from various states. But such harmonization clearly goes beyond those legal requirements, which suggests that it must be understood as being in the platforms' interest – even though the extent to which this harmonization may expand beyond dominant internet platforms remains to be seen.

The laws of different states, by contrast, are yet to reach a comparable degree of harmonization. Given how far-reaching cultural, economic, societal, and religious differences impact the fundamental laws of each state, such harmonization seems unlikely.

Interviewed experts also drew attention to the cooperative spirit among the major internet platforms in pursuit of common goals, such as content moderation. As some interviewed experts noted, there is less of a cooperative spirit among states, aside from sectoral cooperation in the context, for example, of law enforcement. In fact, interviewed experts noted a clear trend of individualism among states, with each state prioritizing its own immediate interest over the interest of the global community.

It is also noteworthy that, in relation to some types of content, platforms have taken the lead in setting standards. The move against non-consensual distribution of sexually explicit media is one example of this (Chapter 3.1.4).

In an environment where standard creation is not the exclusive domain of nation states, these differences between harmonized company norms and fractured country-based norm setting may have long-term implications of strong relevance for cross-border legal challenges on the internet.

2.4.3

Judicial cross-fertilization – scalability, replication and imitation

The physical structure of the internet is coordinated to a large extent. Many aspects of the logical layer, such as the domain name sphere, are coordinated, as well. Yet both the literature and stakeholder input provided for this Report suggest that there is a lack of international coordination and cooperation on regulation of the internet more broadly.

A clear majority (68%) of surveyed experts 'strongly disagreed' or 'disagreed' that the existing tools of inter-state legal cooperation are effectively addressing online abuses. Only 2% 'agreed' or 'strongly agreed', while 30% responded that they 'neither agreed nor disagreed'.

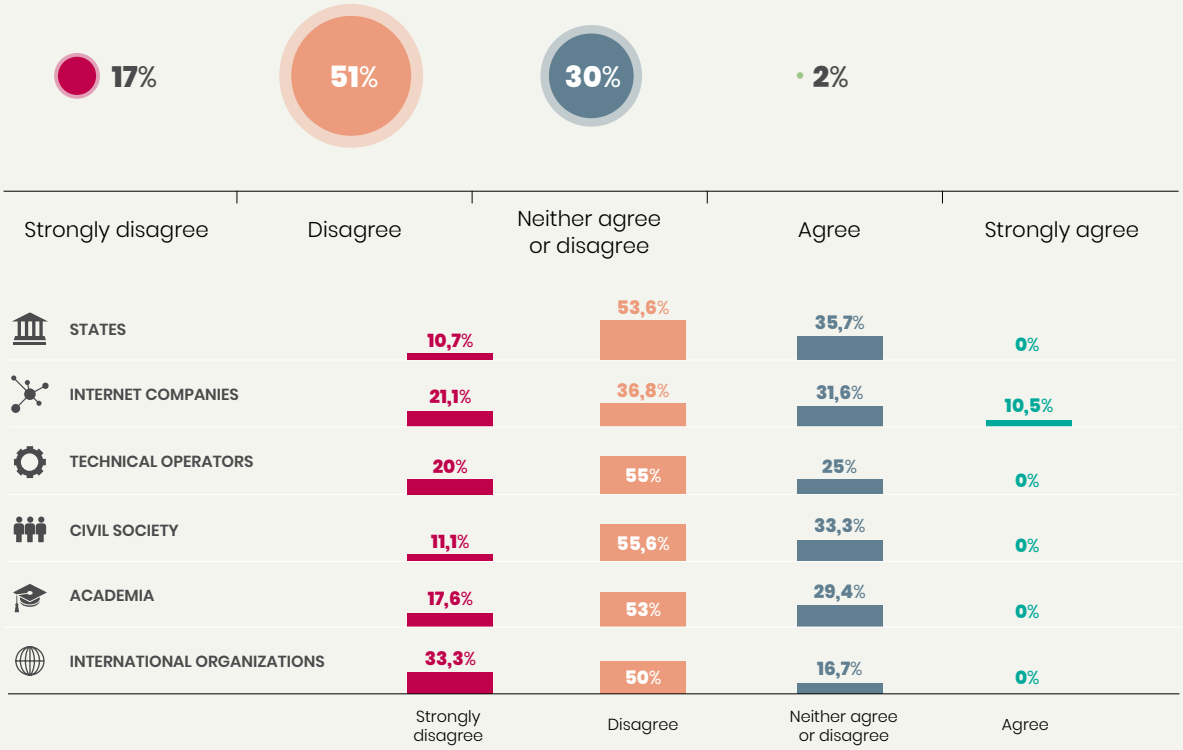
The responses highlighted consensus across regions and stakeholder groups, and several important comments from surveyed experts substantiate concerns held throughout the ecosystem. For example, one surveyed expert noted that tools alone cannot address online abuses, and that effective mitigation requires (1) an awareness of the available tools, and (2) the skills to use them. Furthermore, several surveyed experts stressed that although existing tools of inter-state legal cooperation may be sufficient for non-urgent matters, slow bureaucratic procedures are a bad fit with the rapid pace of the internet.

In their comments on the existing tools of inter-state legal cooperation, surveyed experts also emphasized the need for a multistakeholder approach (Chapter 1.10). For example, one comment noted that it is not only governments that need to work together, but business and civil society, as well. At the same time, several surveyed experts commented that although there is still a long way to go, improvements are noticeable.

The lack of coordination is a direct, and perhaps natural, consequence of the fact that states enjoy sovereignty insofar as they have the capacity to make their own laws. Given that states take fundamentally different approaches to matters such as balancing human rights, protecting consumers and supporting business, it is not surprising to see problems in coordinating internet regulation. Further complicating efforts at coordination are fundamental differences in state attitudes toward the roles that democracy and religion should play in legal matters. The complexity of this situation will only increase as more developing states play bigger roles online. As previously noted, the international climate has also changed more broadly in recent years, as states move away from international collaborative efforts and common goals, and toward more inward-looking policies that prioritize the immediate interests of each state. To put it

INFOGRAPHIC 11

Do existing inter-state legal cooperation tools effectively address online abuse?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

simply, international distrust seems to be increasing. This broader political trend inevitably presents an additional hurdle for the effective coordination of internet regulation.

At the same time, it remains a fact that, due to the cross-border nature of the internet, the challenges faced online can only be addressed through international collaborative efforts and the pursuit of common goals; stakeholders simply cannot afford to not collaborate. An individual state neither can, nor should, control the internet or what is available online. For the moment, international multistakeholder dialogue remains the only alternative.

However, there are numerous indicators that the world is not ready for a general international agreement to settle all matters of internet regulation. Such a giant leap is unfortunately unrealistic. Instead, progress will be achieved through many small steps, at least for now. States could increase efforts to identify uniting features and to iron out at least the most serious inconsistencies and clashes between domestic legal systems, in relation to both substantive and procedural law. In this context, interviewed experts noted that although harmonization may currently be impossible on some topics, greater harmonization seems both possible and valuable on other topics (e.g., data breach notification schemes).

Hints of the 'small step' progress discussed above can be seen in the emergence of global jurisprudence via judicial cross-fertilization. Simply put, courts and regulators are increasingly heeding, copying and imitating approaches taken by foreign courts. Examples of this are prominent in the data privacy field, where the EU's GDPR (Chapter 3.1.6.1) is being widely copied and imitated.

As discussed in more detail below, judicial cross-fertilization is by no means occurring in an evenhanded manner. In many instances, the influence is unidirectional rather than mutual – typically from industrialized states to developing states.

More broadly, this judicial cross-fertilization acts as a 'double-edged sword'. In cases where the approach adopted from another state works toward increased international harmonization, imitating that approach may obviously have a positive impact. But in cases where the approach adopted from another state is aggressive in nature, each adoption of that approach into a new legal system moves us further from solutions to the cross-border issues faced online. Not all approaches are scalable, either. Courts and other lawmakers should always bear this in mind, both when selecting how they approach a specific legal issue, and when deciding which, if any, approaches from foreign courts or lawmakers to adopt. Indeed, it is arguably reasonable to expect lawmakers in those countries that commonly influence policy and law developments globally to conduct what may be termed a 'global south impact assessment', assessing: (1) what impact their approaches will have in the global south, and (2) what will happen if the global south adopts their approaches. In addition, courts and other lawmakers ought to bear in mind that the ultimate goal of international law is to help to ensure the survival of the human species, with obvious sub-goals such as ensuring peaceful coexistence, environmental protection and upholding human rights. The internet can play an important role in helping to build international links and relations through cross-border communication and interaction. We must, therefore, avoid using the online environment as a new arena for international conflict. These goals must be integrated into any assessment of internet jurisdiction.

Indeed, it is arguably reasonable to expect lawmakers in those countries that commonly influence policy and law developments globally to conduct what may be termed a 'global south impact assessment', assessing: (1) what impact their approaches will have in the global south, and (2) what will happen if the global south adopts their approaches.

2.4.4

Rules are set for – and by – established large actors

An examination of the survey and interview results points to five factors that, together, make a range of actors – developing countries, smaller countries and smaller internet actors – feel disempowered:

1. There is a perception that, compared to developed countries, developing countries have less of a say in the approaches taken by the major internet actors;
2. There is a perception that, compared to major internet actors, smaller internet actors have less of a say in the approaches taken by the regulators;
3. There is a perception that both smaller internet actors and developing countries lack a voice in the international dialogue;
4. Extraterritoriality allows dominant states to impose their laws on the world, while smaller states lack the standing and means to enforce their laws even domestically; and
5. Legal approaches from developed countries are being replicated to such a degree that it impacts the sovereignty and self-determination of developing countries.

A concern raised by several interviewed and surveyed experts is that much of the discussion around how to tackle the cross-border internet issues centers around the largest internet companies – particularly US-based companies such as Google, Microsoft, Facebook, Apple, Amazon, Twitter and eBay. There are non-Western examples of this dynamic, as well; Chinese standards, for instance, are introduced as a *de facto* component of subsidized mobile and terrestrial broadband infrastructure projects in parts of Africa. This leads to a skewed perspective of the issues faced by the great majority of internet actors, which consists of smaller businesses and organizations. In fact, large actors may also be at a disadvantage in dialogues where they have a structure or business model that deviates from the more standardized structures of the major actors. For example, Wikipedia operates across borders and is available in different versions, like other major internet platforms. However, the various Wikipedia versions are language-based and independent from one another – which is distinctly different from the more standard approach of publishing different country versions of a platform. The implications of this structural difference are profound. In the context of content removal orders, for example, a court order to remove certain content will inevitably affect all users of the Wikipedia language version in question, and removal on one language version has no impact on what is available on another language version. Courts and regulators need to be alert to the legal implications of

these type of structural differences.

There are obvious and practical reasons for directing the most attention at the major internet platforms. Where governments wish to maximize impact, they naturally target companies with the greatest number of users. And the major internet companies have the resources to participate in discussions on matters of internet regulation. Yet, despite such practical justifications, the under-representation of smaller internet players remains an overarching meta-trend that ought to be addressed. Further, constructing solutions based on the regulation of the major technology companies may not be an effective way to address undesirable conduct by smaller actors operating under markedly differently conditions.

Highlighting another meta-trend, many interviewed and surveyed experts from developing countries (and, to a degree, from smaller countries) perceived that they become aware of, and participate in, important policy and regulatory discussions only when many decisions have already been made. This is partially an issue of access to information and is discussed in more detail elsewhere in this Report (Chapter 2.2.4).

There is a continuing need to work on solutions for soliciting and incorporating early input from all stakeholders. The under-representation of smaller internet actors and developing countries in crafting solutions requires both re-thinking and restructuring. Increased capacity building is one of the more obvious responses.

There is also a power imbalance in the context of the extraterritorial application of laws. Some states have greater power to have their laws enforced in an extraterritorial manner, even in cases where the laws in question are identical, or near identical. This power imbalance – often between industrialized and developing countries – may become increasingly visible as more states adopt 'rep localization' requirements, discussed in Chapter 4.1.3.

> "The under-representation of smaller internet actors and developing countries in crafting solutions requires both rethinking and restructuring."

2.5

New roles for intermediaries

Without internet intermediaries such as search engines, auctioning platforms, video platforms and social media platforms, the internet would be considerably less useful, and considerably less user-friendly. Indeed, internet intermediaries play a central role in the operation of the online environment; they have in the past, they do so now, and they will continue to do so in the future.

2.5.1

Increasing responsibility bestowed on private operators

The exact roles and responsibilities of internet intermediaries are contested and controversial topics, and the subject of extensive and detailed work. The Stanford World Intermediary Liability Map, for example, is an online resource that provides internet platforms and others with information on online liability laws.[74] The increasing responsibility bestowed on private operators – through laws that make internet platforms the gatekeepers of content, as well as the voluntary assumption of responsibility – has occurred in numerous fields. This trend is particularly discernable in certain fields and has evolved particularly far in the context of terrorism, extremism and hate speech – fields in which some laws demand fast response times in content blocking. For example, on December 19, 2018, Facebook announced that it had banned 425 pages, 17 groups, 135 Facebook accounts and 15 Instagram accounts for engaging in coordinated inauthentic behavior linked to the situation in Myanmar.[75] The banned accounts were sharing anti-Rohingya messages – the same kind of messages that

74. Stanford Center for Internet and Society. (2018). *World intermediary liability map*. Retrieved from https://wilmap.law.stanford.edu/.

75. Internet & Jurisdiction Policy Network. (2018, December). Facebook announces ban of over 400 pages and 100 accounts relating to Myanmar conflict. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7741_2018-12.

have fueled a broader genocide in Myanmar.[76] The ability for Facebook to remove pages that do not comply with its terms of service was confirmed by the US District Court in a recent First Amendment case brought by a Russian plaintiff (the Federal Agency of News).[77] As far as extremism and hate speech are concerned, one of the most widely noted frameworks is the May 2019 *Christchurch Call*.[78]

Another noteworthy instrument, one specifically aimed at increasing the responsibility bestowed on private operators, is the 2016 *Code of conduct on countering illegal hate speech online* presented by the EU Commission, together with Facebook, Microsoft, Twitter and YouTube. Under this arrangement, the mentioned IT companies undertake to:

- Have in place clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content.
- Have in place Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct.
- Upon receipt of a valid removal notification, review such requests against their rules and community guidelines and, where necessary, national laws transposing the Framework Decision 2008/913/JHA, with dedicated teams reviewing requests.
- Review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.

The cross-border implications are obvious.

2.5.2

(In)voluntary gatekeepers

The role of – and possible protection for – internet intermediaries is often approached from extremist points of view. Some seek to impose an uncompromising free speech regime, under which internet intermediaries impose no restrictions on what internet users upload. Others see internet intermediaries as little more than useful tools for government control of internet content and activities. Such extreme views are ultimately unhelpful, and we need to strive for an appropriate balance.

Historically, Western countries have viewed internet intermediaries as crucial for the development of the internet, and have therefore afforded them extensive protection – for example, in the form of the well-known §230 of the US *Communications Decency Act* of 1996 and through Articles 12-15 of the EU's *E-Commerce Directive*.[79] Both of these instruments provide internet intermediaries with protection against liability in certain circumstances. But this attitude seems to be changing.

In focusing on cross-border legal challenges on the internet in relation to internet intermediaries, at least five key issues must be addressed as a matter of urgency:

1. The need to minimize, or preferably eliminate, situations where internet intermediaries risk violating one state's law by complying with another state's law;
2. The need to clarify the extent to which internet intermediaries – as private actors – may assume the role of fulfilling quasi-judicial functions (either voluntarily or involuntarily);
3. The need to clarify a framework for how internet intermediaries should determine the geographical scope of jurisdiction (Chapter 4.1.7) when they block or remove content;
4. The need to ensure that the law provides the clearest possible guidance as to what is expected of the internet intermediaries; and
5. The need for clear distinctions between situations where internet intermediaries are viewed as publishers and where they are seen as neutral platforms.

Situations where a party risks violating one state's law by complying with another state's law are referred to as 'true' conflicts of laws. There is widespread recognition that they benefit no one and should be avoided. The problem is finding a way to do so in a climate where states are rarely willing to compromise on the applicability of their laws.

A potential model can be found in Australia's *Privacy Act*. Section 6A limits the extraterritorial effect of the Act by providing that: "[a]n act or practice

---

76. Wagner. K. (2018, December 18). Facebook removed hundreds more accounts linked to the Myanmar military for posting hate speech and attacks against ethnic minorities. *Recode*. Retrieved from removed-rohingya-genocide.

77. Internet & Jurisdiction Policy Network. (2019, July). US court rules that Facebook is well within its limits to remove pages linked to misinformation campaign. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiZmVkZXJhbCBhZ2VuY3kgb2YgbmV3cyIsImZyb20iOilyMDEyLTAyIiwidG8iOilyMDE5LTA5In0=.

78. Christchurch Call. (2019). Retrieved from https://www.christchurchcall.com/.

79. Directive (EC) 2000/ 31 of the European Parliament and Council, 8 June 2000, on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce [2000] OJ L178/ 1, 369.

does not breach an Australian Privacy Principle if: (a) the act is done, or the practice is engaged in, outside Australia and the external Territories; and (b) the act or practice is required by an applicable law of a foreign country."[80]

The duties-focused definition of conflicts of laws only describes part of the problem. There are also so-called 'false' conflicts of laws. These occur when a person subject to two or more laws can comply with all the applicable laws, which can be the case if one law is more flexible than the other, or if one law gives a right and the other imposes an opposing duty.

In the context of internet intermediaries, the importance of such 'false' conflicts of laws may have been underappreciated. The correlative relationship between rights and duties, familiar to us from domestic law, does not exist in the cross-border environment; rights provided under one state's legal system may not necessarily create corresponding duties under another legal system. To assess whether two (or more) laws are in conflict, we need to account for both the duties and the rights for which those laws provide. In other words, even where duties do not clash, but the rights of one country clash with the duties of another state, we need to carefully evaluate to which law priority is given. In an international context, there are no overarching legal reasons for an internet intermediary to automatically prioritize duties imposed by one state over the rights afforded by other states. On a practical level, however, internet intermediaries may seek to avoid penalties by abiding by the duties imposed by one state rather than pursuing the rights afforded under the law of other states, unless they receive safeguards. This leads to a risk of over-blocking and a race to the bottom.[81]

Internet intermediaries fulfill quasi-judicial functions in a variety of contexts. Sometimes this happens voluntarily, and sometimes this role is forced upon them. Examples of the former include actions such as the removal of child abuse material. On October 24, 2018, for example, Facebook announced that it had removed 8.7 million child abuse images in the previous three months, using previously undisclosed software that helps flag potential child abuse material for its reviewers.[82]

> "Internet intermediaries fulfill quasi-judicial functions in a variety of contexts."

An observation made by one inter viewed expert is particularly pertinent in this context. Perhaps due to the company structure commonly adopted by major US internet platforms, and perhaps out of convenience, decisions relating to content blocking and takedowns are often implemented on a regional, rather than national basis in some parts of the world. For example, if one country in the Middle East orders content to be blocked or taken down due to blasphemy laws, that content is frequently blocked or removed for the entire region – even though the content in question may well be lawful in some countries in the region.

There are many examples of internet intermediaries being forced to assume a quasi-judicial function. For example, on December 6, 2018, Ugandan internet service providers (ISPs) started implementing a directive of the Uganda Communications Commission (UCC) to block access to websites with adult content;[83] examples from China, Indonesia, Korea, Russia, Turkey as well as Australia and the EU are mentioned later in the Report.

In these situations, internet intermediaries become the censors and gatekeepers of speech – a role for which they are typically ill suited. It is questionable whether society should assign such a crucial role to private entities.

Some may point to the fact that newspapers, radio and TV broadcasters have long acted as censors in deciding what content to make available. But the role of the internet intermediary is so fundamentally different that one cannot, and should not, draw such a comparison. A common argument holds that internet intermediaries are more like the postal service, passively distributing other people's content without interference. Yet, such analogies may only serve as a distraction, rather than providing a useful tool for discussion. The reality is that no intermediaries in history have had to manage the volume of user-generated content that internet intermediaries do today.

The role of internet intermediaries must therefore be approached with fresh eyes, free from preconceived notions based on comparisons with the roles of offline intermediaries.

Expectations of internet intermediaries only serve to complicate the situation. While most people would expect internet intermediaries to abide by the law of their respective countries, they would probably not want them to abide by all laws of *all* other countries in the

---

80. Privacy Act 1988 (Cth), s 6A(4).

81. PwC. (2018). *Top policy trends of 2018*. Retrieved from https://www.pwc.com/us/en/services/consulting/risk-regulatory/top-policy-trends-2018.html.

82. Internet & Jurisdiction Policy Network. (2018, October). Facebook announces it has removed 8.7 million child abuse images in past three months thanks to previously undisclosed software. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7567_2018-10.

83. Internet & Jurisdiction Policy Network. (2018, December). Uganda: ISPs start implementing regulator's order to remove access to websites with adult content. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7736_2018-12.

world. In the end, such compliance would force internet intermediaries to prioritize the most restrictive laws from all the countries in the world. Such a 'race to the bottom' is certainly an unhealthy direction for the internet. And if this is undesired, there is a need to consider whether a globally active internet intermediary can ever be excused for not complying with all the laws around the world that claim to apply to its conduct. If stakeholders answer that question in the affirmative, how should a globally active internet intermediary decide which laws to abide by? These are, to a degree, novel questions in international law.

Without clear guidance from the law, internet intermediaries may be tasked with deciding the legality of certain content.[84] In such a situation, one could argue that internet intermediaries are set up to fail due to the vagueness of the laws they must apply. It may also be noted, in this context, that internet intermediaries are tasked with fulfilling such quasi-judicial functions at a fast pace. While the judiciary may take months or even years to reach a decision on a certain matter, internet intermediaries may be required to decide the same matter in minutes given the volume of decisions it needs to make.

Because it may be difficult to identify and bring to justice the party responsible for specific online activities, litigants and regulators may be tempted to target the internet intermediary used for those activities, instead. Justice Fenlon made this point very clearly in the aforementioned Canadian *Equustek* case, stating: "Google is an innocent bystander but it is unwittingly facilitating the defendants' ongoing breaches of this Court's orders. There is no other practical way for the defendants' website sales to be stopped."[85] Justice Fenlon's message is clear: where the legal system fails, internet intermediaries can expect to become the scapegoats of choice.

There is also a long-standing issue of distinguishing between internet intermediaries as publishers and internet intermediaries as neutral platforms. Obviously, protections for neutral platforms may not extend to situations where internet intermediaries act as publishers. This crucial neutrality is undermined when platforms are required to promote specific narratives, as was the case in the 2016 European Union *Code of Conduct* on countering illegal hate speech online (Chapter 3.1.1). In this context, it has been noted that: "While the promotion of counter-narratives may be attractive in the face of 'extremist' or 'terrorist' content, pressure for such approaches runs the risk of transforming platforms into carriers of propaganda well beyond established areas of legitimate concern."[86]

One interviewed expert considered that through mergers, acquisitions and growth, many intermediaries are changing functions to the extent that within the same company, there may be an advertiser, brand holder, registrar and publisher, and that this creates an interesting tension. Another interviewed expert commented that intermediaries are faced with many different jurisdictions and associated rules that pose a significant challenge – not only for their compliance with those rules, but for communicating how they apply those rules.

Yet, another interviewed expert saw this aspect as leading to the vesting of significant power in those companies to implement solutions. That is, if these companies implement localized solutions on certain issues, it may lead to a more fragmented internet with different rules that apply in different places. This expert was concerned about the lack of ability for smaller players, including businesses and small countries, to influence the larger intermediaries in the implementation of policies. Indeed, as one interviewed expert stressed, this issue also extends to mid-level powers who enact policies that large platforms largely ignore, unless they fit with the current approaches of the biggest countries. There are also cases where social media platforms are used by governments to force their values onto persons in other states. For example, Chinese-owned social media app TikTok now bans pro-LGBT content even in countries where homosexuality has never been illegal.[87]

Such actions have far-reaching consequences. At the minimum, it likely undermines the popularity of the affected social media.

One final observation may be appropriate. In all this we must realize that as governments divert responsibilities and decision making to the online platforms, making them the Internet's gatekeepers, governments are also transferring power to these platforms. This may undermine accountability, transparency and ultimately, justice.

---

84. Sartor, G. (2013). Provider's liability and the right to be forgotten. In Svantesson, D. & Greenstein, S. (Eds). *Nordic yearbook of law and informatics 2010– 2012: Internationalisation of law in the digital information society*. Copenhagen: Ex Tuto Publishing. 101– 37, 111.

85. Equustek Solutions Inc. v. Jack, 2014 BCSC 1063, para 156. In addition, Fenlon J's assertion that there is no other practical way for the defendants' website sales to be stopped seems misguided, as e.g. also the relevant defendant's payment channels could have been targeted.

86. United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom and Expression. (2018) 2018 T*hematic Report to the Human Rights Council*. A/HRC/38/35. Retrieved from http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35, p. 8.

87. Hern, A. (2019, September 26). TikTok's local moderation guidelines ban pro-LGBT content. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/sep/26/tiktoks-local-moderation-guidelines-ban-pro-lgbt-content.

2.5.3

Appeals and recourse become key issues

When a court or an authority decides a matter, it is typically possible to appeal the decision, and to gain an insight into the reasoning that led to the decision. Such a transparent appeals mechanism is currently lacking in situations where a private actor acts as the decision maker. This is a serious consideration in a context where private operators have increased responsibility to act as filters of speech.

Having said this, it should of course be acknowledged that any decision made by an internet intermediary may be challenged before the courts. This may provide some comfort. However, such a process is typically not an efficient response to perceived injustices and may often involve complex jurisdictional questions.

As one interviewed expert noted, the lack of grievance resolution mechanisms and the need for transparency among platforms are being discussed as part of the UN Internet Governance Forum's Dynamic Coalition on Platform Responsibility.[88] This expert noted that the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur on FOE) also recommended, in a 2018 Thematic Report to the United Nations Human Rights Council, that companies improve their transparency and accountability in content regulation.[89]

It should be noted that many of the larger internet companies issue transparency reports. But as observed by one interviewed expert, while those reports include aggregate numbers of content takedowns, they do not currently provide nuanced details about how decisions are being made.[90] On the topic of transparency, one interviewed expert said that companies have not successfully found a way to communicate the details of their internal procedures and how they apply different rules. This failure has provoked a normative backlash by governments, particularly in the context of hate speech and fake news.

The issue of accountability is receiving more attention, as well. The Institute for Accountability in the Digital Age (I4ADA), for example, was founded with the mission to ensure that online breaches of norms and values do not undermine the internet's potential to increase access to knowledge, spread global tolerance and understanding, and promote sustainable prosperity.[91] To that end, I4ADA is working on a set of principles – the *Hague Global Principles for Accountability in the Digital Age*[92] – with significant implications for the cross-border legal challenges on the internet.

---

88. Internet Governance Forum. *Dynamic Coalition on Platform Responsibility*. Retrieved from https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-platform-responsibility-dcpr. See also initiatives such as: Internet Policy Observatory. The Santa Clara Principles on Transparency and Content Moderation. Retrieved from https://santaclaraprinciples.org and Manila Principles on Intermediary Liability. Retrieved from https://www.manilaprinciples.org/.

89. United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom and Expression. (2018). *2018 Thematic Report to the Human Rights Council.* A/HRC/38/35. Retrieved from https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ContentRegulation.aspx.

90. See further the work of: Ranking Digital Rights. Retrieved from https://rankingdigitalrights.org/.

91. Institute for Accountability in the Digital Age. Retrieved from https://i4ada.org/.

92. Institute for Accountability in the Digital Age. (2018). *The Hague Global Principles for Accountability in the Digital Age*. Retrieved from https://i4ada.org/wp-content/uploads/2018/06/TheHaguePrinciples_public_consultation-v0.1.pdf.

03

TOPICAL TRENDS

—

EXPRESSION

SECURITY

ECONOMY

Concerns regarding jurisdictional tensions in cyberspace are widespread as the cross-border nature of the internet conflicts with the patchwork of territorially bound national laws. The high degree of legal uncertainty increases the cost of doing business and creates challenges for governments seeking to protect their citizens and ensure respect for their laws. It may also prevent internet users from accessing as broad a range of content, as they otherwise could, and raises civil society concerns that abuses are not properly addressed, or that attempted solutions will harm users. Addressing these concerns is a matter of urgency.

To understand the details and full complexity of cross-border legal challenges on the internet, it is useful to map out the major trends within the topics that are most relevant to the Internet & Jurisdiction Policy Network's stakeholder groups.

To this end, this Chapter aims to highlight a selection of particularly significant 'trends' within topics ranging from data privacy to taxation, and from the Internet of Things to cybercrime. These diverse topics have been grouped into three broader categories:

1. Expression
2. Security
3. Economy

While this approach should aid the clarity of the presentation, some topics may fit into more than one category. There are also obvious points of connection and indeed overlap across these categories. For example, economic interdependence among states remains a check on aggressive behavior,[93] which highlights the link between security and economy.

Within each of the discussed topics, more detailed attention is given to particularly important trends as identified through the survey results, interviews and extensive desk research, including an analysis of the Internet & Jurisdiction Policy Network's wide-ranging collection of relevant trends and developments available in the I&J Retrospect Database.[94]

These sources have also made it possible to briefly outline other significant trends within each topic area. The goal is to be comprehensive without necessarily being exhaustive. While it is, therefore, obvious that additional trends could have been incorporated,[95] the working goal has been to ensure a high probability that the Internet & Jurisdiction Policy Network's stakeholders agree that all included trends are of significance.

---

93. Office of the Director of National Intelligence. (2017). *Global trends: Paradox of progress.* Retrieved from https://www.dni.gov/index.php/global-trends/near-future.

94. Internet & Jurisdiction Policy Network. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect.

95. There are some major jurisdictional trends left out in this section that are likely to gain much more attention within a foreseeable future. For example, one surveyed expert brought attention to the jurisdictional dimension of the environmental costs that technological growth incurs (for one example see Chapter 3.3.5). And as pointed out by one interviewed expert, another such matter is found in that there is an increasing concern about digital labor issues. For example, persons employed to assess take-down request are becoming an integral part of the internet infrastructure doing menial tasks that greatly impact freedom of expression. Cross-border issues arise where such tasks are allocated to foreign workers, and questions have arisen as to the degree of support afforded to such workers who often are exposed to highly disturbing and offensive content. Issues such as this are important but have not been included in this year's Report.

3.1

Expression

The first category of major topical trends concerns expression. Recent discussions around the intersection of internet, jurisdiction and expression have focused on concerns about hate speech, extremism and fake news, as well as the widespread reform of data privacy regimes around the world. Increasingly, broad claims pervade these discussions, and there is a growing appetite amongst regulators to re-examine the roles, and responsibilities, of internet intermediaries.

Encouraging and facilitating cross-border expression has been a driving force behind much of the internet's development, both in physical (e.g., hardware) and non-physical (e.g., content platforms) dimensions. As many critical early developments originated in the US, the American perspective on freedom of speech – most prominently articulated in the First Amendment to the US Constitution – has colored much of the early discourse and guiding principles.[96] While weaker today due to the strong proliferation of internet usage outside the US – where, for example, more than 80% of Facebook's users now reside – the encouragement and facilitation of freedom of expression, including cross-border expression, remains a valued cornerstone of the internet in large parts of the world. In recognition of this, the UN has stressed that the right to freedom of expression on the internet is an issue of increasing importance.[97]

The importance of cross-border expression

When asked what, if any, negative consequences they foresee if cross-border legal challenges on the internet are not properly addressed, 59% of surveyed experts raised the issue of potential restrictions on expression. This was one of the strongest concerns among the stakeholders.

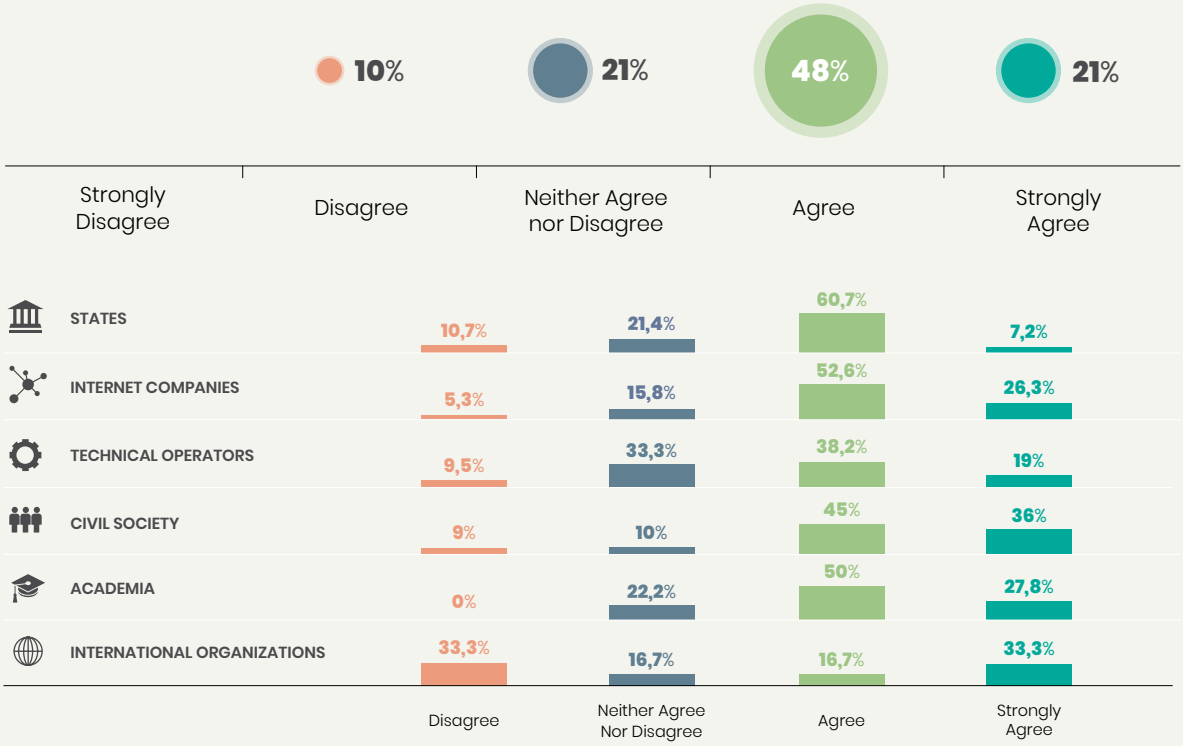
---

96. U.S. Const. amend. I. Retrieved from https://constitutioncenter.org/interactive-constitution/amendments/amendment-i.

97. See e.g.: United Nations, General Assembly. *Human Rights Council: Draft Resolution: The promotion, protection and enjoyment of human rights on the internet*, A/HRC/32/L.20 (June 27, 2016). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

INFOGRAPHIC 12

Are cross-border legal challenges on the internet a significant barrier for Small and Medium Enterprises (SMEs)?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Freedom of expression is a fundamental human right – both offline and online[98] – and it is protected in several international human rights instruments, as well as in the domestic law of many states. However, freedom of expression is one of several fundamental human rights and must be viewed as part of a system of rights that sometimes have to be reconciled, or balanced. This is highlighted in works such as the Council of Europe's Guide to Human Rights for Internet Users, adopted in April 2014.[99] The Guide outlines the basic framework of principles to protect the fundamental human rights guaranteed by the European Convention on Human Rights for all internet users.

Among the many states that value freedom of expression, there is a great diversity as to when they see it as appropriate to have other, competing, rights counterbalance freedom of expression.[100] The *Yahoo! France* case, dating back to the year 2000[101], is the most illustrative – and foundational – internet jurisdiction dispute to date.

While the *Yahoo!* case involved a transatlantic dispute, the difference in attitudes toward freedom of expression vary even more greatly on a global level. It must be emphasized

98. United Nations, General Assembly, *Human Rights Council: Draft Resolution: The promotion, protection and enjoyment of human rights on the internet*, A/HRC/32/L.20 (June 27, 2016). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement, p. 3.

99. Council of Europe. (2014). *Guide to human rights for internet users*. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31.

100. See further: Oster, J. (2017). Which limits on freedom of expression are legitimate? Divergence of free speech values in Europe and the United States. In: Kohl, U. (Ed.). *The net and the nation state*. Cambridge, United Kingdom: Cambridge University Press, 39-47.

101. International League Against Racism & Anti- Semitism (LICRA) v Yahoo! Inc and Yahoo! France [2000] Tribunal de Grande Instance de Paris (County Court of Paris).

that the challenges of upholding freedom of expression online vary, in both degree and nature, across countries and regions. As some surveyed and interviewed experts pointed out, this varies, in part, according to different distinctions between religious and political power. The Pakistan Telecommunication Authority (PTA), for example, announced in October 2017 that it would form a high-level committee to monitor and block blasphemous content online.[102] The content of concern to the PTA is perfectly legal in most parts of the world, and may indeed be protected speech in many states. The question, then, is to what extent laws such as Pakistan's religious laws can and should influence the availability of such content online.

Similar questions of one state's speech restrictions influencing the availability of content in other states arise, for example, around the EU's 'right to de-referencing' (Chapter 3.1.6.2), US copyright law (Chapter 3.3.1.2), or Chinese restrictions on images of Winnie the Pooh.[103]

> "Realizing just how different the freedom of expression situation is around the world is a necessary first step toward protecting cross-border internet expression."

Addressing these questions is a necessity and must be a political priority worldwide. A 2018 report from Freedom House notes that political rights and civil liberties around the world deteriorated to their lowest point in more than a decade in 2017, and that only 39% of the world's population live in countries that the study classifies as 'free'.[104] As the late journalist Jamal Khashoggi noted in his very last column:

> "Arab governments have been given free rein to continue silencing the media at an increasing rate. There was a time when journalists believed the internet would liberate information from the censorship and control associated with print media. But these governments, whose very existence relies on the control of information, have aggressively blocked the internet. They have also arrested local reporters and pressured advertisers to harm the revenue of specific publications."[105]

The same may be said about other regions, and as emphasized by one surveyed expert, there can be no doubt that laws, policies and various cooperative measures may either empower or hurt cross-border journalism.

Realizing just how different the freedom of expression situation is around the world is a necessary first step toward protecting cross-border internet expression. It should be noted that even within comparatively homogenous legal blocks, such as the EU, there are considerable differences when it comes to freedom of expression.[106] There may also be differences of opinion within a state, as evidenced by recent federal challenges to California's net neutrality law.[107]

This diversity across states has far-reaching implications. On its most basic level, it means that any speech-related matter where the court in one state claims jurisdiction to adjudicate for another, represents that state's approach being prioritized over the values of the other state. Even where this is justified by referencing procedural efficiency, it still undermines fairness and due process, and may in fact have negative implications on international relations.

Interview and survey responses highlighted concerns about the risk of a 'race to the bottom'. There is a real possibility that countries with the most restrictive views will impose those views on the rest of the world, leading to a global set of restrictions that are incompatible with the freedom of expression rights in other countries.

At the same time, partially due to the rise of artificial intelligence, the internet risks being flooded with undesirable online content such as hate speech, bullying and deep fakes to the extent that its value as a communications medium is undermined. Such a 'junkification of the internet' would be highly destructive and must be avoided.

In discussing freedom of expression, it must also be noted that restrictions

---

102. Dawn. (2017, October 25). *Body to block blasphemous content on internet*. Retrieved from https://www.dawn.com/news/1366064/body-to-block-blasphemous-content-on-internet.

103. McDonell, S. (2017, 17 July). *Why China censors banned Winnie the Pooh*. Retrieved from https://www.bbc.com/news/blogs-china-blog-40627855.

104. Freedom House. (2018). F*reedom in the world 2018*. Retrieved from https://freedomhouse.org/report/freedom-world/freedom-world-2018.

105. Khashoggi, J. (2018, October 17). What the Arab world needs most is free expression. *The Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/global-opinions/jamal-khashoggi-what-the-arab-world-needs-most-is-free-expression/2018/10/17/adfc8c44-d21d-11e8-8c22-fa2ef74bd6d6_story.html?noredirect=on&utm_term=.4d5fab2ea101.

106. In fact, Art. 1(2)(g) of the *Rome II Regulation* (Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations) that determines the applicable law in non-contractual obligations excludes such obligations "arising out of violations of privacy and rights relating to personality, including defamation" from that Regulation. This exclusion is a direct result of the considerable differences that exist in the balancing between freedom of expression and the right to reputation amongst the Member States of the European Union.

107. Electronic Frontier Foundation. (2018, October 1). *California's net neutrality law: What's happened, What's next*. Retrieved from https://www.eff.org/deeplinks/2018/10/californias-net-neutrality-law-whats-happened-whats-next.

that are generally appropriate may be inappropriate for particular actors. Libraries, for example, may be tasked with archiving and preserving materials – for research and education purposes as well as for ensuring accurate historic records – that generally may not be communicated. In this context, one expert noted that a common theme is the fact that while the internet has enabled many of the activities that libraries themselves have long looked to promote, internet regulation and corporate practice can restrict them. The jurisdictional dimension is obvious. Through holding materials that are accessed across borders, and by facilitating users accessing materials held elsewhere, libraries are exposed to complex cross-border legal issues that they may not be well placed to deal with. A key challenge is to ensure that in any decision-making about whether and how to control information flows, the impacts on users around the world is taken into account.

3.1.1

Extremism, terrorism and hate speech

The regulation of extremism and hate speech is particularly complex in cross-border situations. First, there is no worldwide agreement as to what amounts to hate speech or extremism. Further, as the saying goes, one man's freedom fighter is another man's terrorist. Therefore, there can be no general agreement around what amounts to the promotion of terrorism. Practical complications of jurisdiction and enforcement also arise where content is created and uploaded in one state, hosted in a second state and accessed in a third, as often is the case with these types of content.

The aforementioned *Yahoo! France*[108] case is illustrative in this context. It involved a US company, Yahoo!, operating a website that, among other things, contained an auction service where Nazi material was on offer. Making such material available for sale was legal in the US, but contrary to the French penal code. Following a complaint by two French organizations, a French court ruled against Yahoo! and issued a civil law injunction based on the French *Code of Civil Procedure*. However, a US court subsequently granted Yahoo! a summary judgment to the effect that US courts would not enforce the French decision.[109]

Although it is a longstanding issue, the fundamental clash of attitudes apparent in the French *Yahoo!* case has slowed progress on the regulation of cross-border extremism and hate speech.

There are suggestions that the promotion of extremism, terrorism and hate speech is on the rise online, and the internet has indeed proven to be a fertile ground for the distribution of such content. Some surveyed and interviewed experts indicated that 'hate activities' are increasing in general, and that what happens offline typically is mirrored online.

Other surveyed and interviewed experts suggested that issues such as hate speech and fake news may not necessarily be increasing, and that there is only more discussion about them. This, together with increased transparency, may result in overestimating the increase, or even an increase in 'anxiety and hysteria' around these issues. One interviewed expert also noted that there is a divide between what politicians say about hate speech on the one hand, and actual legislative initiatives on the other. This is an important point, as political calls for stricter laws in response to tragic events, such as terrorist acts, commonly neglect the fact that it is those same politicians that are entrusted to enact such laws whom have failed to do so.

Nevertheless, some states have taken various steps to fight the distribution of extremism and hate speech, with several passing laws specifically on the topic. Germany's Enforcement on Social Networks Law of 2017 (or *Netzwerkdurchsetzungsgesetz*, NetzDG), has gained considerable attention and requires social networks to remove hate speech or criminal content and to report on the number of illegal content complaints received. Facebook was subsequently fined by Germany for underreporting its illegal content complaints.[110] A similar law was passed by France in July 2019, requiring platforms to remove 'obviously hateful' content within 24 hours.[111] And on July 13, 2018, Zambia's Communication Minister announced that the govern-

---

108. International League Against Racism & Anti- Semitism (LICRA) v Yahoo! Inc and Yahoo! France [2000] Tribunal de Grande Instance de Paris (County Court of Paris).

109. Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme [2001] NDCal 169 F Supp 2d 1181. See, also, Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme [2006] 9th Cir 433 F3d 1199.

110. Gold, H. (2019, 2 July). Germany fines Facebook for under-reporting illegal content. *CNN Business*. Retrieved from https://edition.cnn.com/2019/07/02/tech/facebook-germany-illegal-content/index.html.

111. Internet & Jurisdiction Policy Network. (2019, July). France passes a new law requiring platforms to remove hate speech within 24 hours. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiZnJhbmNlIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDcifQ==.

ment would introduce laws to regulate social media use in order to fight against hate speech, identity theft and pornographic content.[112] The Minister stated the laws would enter into force in 2019.[113] These are merely three examples of a broader trend unfolding in both developing and developed countries. In 2019, Australia amended the Criminal Code specifically targeting the sharing of abhorrent violent material.[114] A particular challenge in drafting such laws, is ensuring that appropriate exemptions are included, for example, for research purposes.[115]

There are also initiatives directed specifically at terrorism-related content. For example, on February 6, 2017, the Israeli Minister of Justice claimed that the government's efforts in combating the spread of terrorist content were finally bearing fruit; internet platforms had partially or fully complied with 1,400 content removal requests since 2016.[116] The Minister also proposed introducing legislation that would impose heavy fines on platforms that fail to remove content inciting violence.[117]

In February 2019, the United Kingdom passed the Counter-Terrorism and Border Security Act 2019,[118] which (among other regulations) criminalizes viewing or otherwise accessing online content likely to be useful in preparing a terrorist act. However, exceptions are made for journalistic and academic activities, as well as people having no knowledge of, or reason to believe, that the materials would contain such content. Furthermore, one surveyed expert brought attention to how in June 2019, the OSCE Representative on Freedom of the Media issued a review of the Albania's draft Law on Audiovisual Media and the Law of Electronic Communications, addressing (among other things) the proposed measures addressing online content inspiring terrorist acts and the potential impacts on freedom of expression and related concerns. The office of the Representative was part of a larger consultation between the Representative's office and the Albanian government. The Representative carries out other work in this area - for instance, organizing the 2019 Central Asia Judicial Dialogue on protecting freedom of expression when combating violent extremism - including extremist content online.

Furthermore, in September 2018, the EU proposed new rules to address online terrorist content. This proposal is noteworthy in that it imposes strict time limits for the removal of terrorist content.[119] The proposal also includes a framework for strengthened cooperation across hosting service providers, Member States and Europol. Within that framework, service providers must designate points of contact, that are available at any time, to follow up on removal orders and referrals.[120] On December 6, 2018, the EU Council adopted its negotiating position on the European Commission's proposal for a regulation against terrorist content online.[121] The position endorses the requirement for cloud providers and internet platform providers to delete terrorist content within an hour, upon receiving orders from law enforcement authorities. In addition, it states that the platforms shall apply certain duties of care to prevent the dissemination of terrorist content on their services, and take proactive measures to address the reappearance of content that had previously been removed.[122] On December 11, 2018, three

---

112. Chutel, L. (2018, 7 July). Zambia is the latest African state trying to muzzle social media with arbitrary laws. *Quartz Africa*. Retrieved from https://qz.com/africa/1322814/zambia-considers-social-media-clampdown-through-new-laws-or-tighter-regulation/.

113. Internet & Jurisdiction Policy Network. (2018, July). Zambia: Government announces regulation of social media to fight against hate speech, identity theft and pornographic content. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7192_2018-07.

114. Attorney General for Australia. (2019, April 4). *Tough new laws to protect Australians from live streaming of violent crimes*. [Press Release], Australia. Retrieved from https://www.attorneygeneral.gov.au/Media/Pages/Tough-New-Laws-to-protect-Australians-from-Live-Streaming-of-Violent-Crimes.aspx.

115. For the Australian Act, see for instance s.474.37(1)(d) of the Criminal Code Act 1995 that provides for access to such material for research purposes.

116. Blum, R. (2017, February 6). Israeli Justice Minister: Efforts to remove terrorism-incitement from social media platforms bearing fruit. *The Algemeiner*. Retrieved from https://www.algemeiner.com/2017/02/06/israeli-justice-minister-at-international-cyber-conference-efforts-of-our-task-force-to-remove-terrorism-incitement-from-social-media-platforms-bearing-fruit/.

117. Internet & Jurisdiction Policy Network. (2017, February). Israeli minister highlights successful content removals, proposes fines against platforms. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-5622_2017-02.

118. Counter-Terrorism and Border Security Act 2019 (UK) c.3. Retrieved from http://www.legislation.gov.uk/ukpga/2019/3/contents.

119. European Commission. (2018, September 12). *State of the Union 2018: Commission proposes new rules to get terrorist content off the web*. [Press Release]. Strasbourg. Retrieved from http://europa.eu/rapid/press-release_IP-18-5561_en.htm.

120. European Commission. (2018, September 12). *State of the Union 2018: Commission proposes new rules to get terrorist content off the web*. [Press Release]. Strasbourg. Retrieved from http://europa.eu/rapid/press-release_IP-18-5561_en.htm.

121. Council of the European Union. (2018, December 6). *Terrorist content online: Council adopts negotiating position on new rules to prevent dissemination*. [Press Release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/.

122. Internet & Jurisdiction Policy Network. (2018, December). EU Council adopts negotiating position on regulation against online terrorist content, endorsing one-hour takedown upon notice and proactive measures against content reappearance. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7726_2018-12.

UN Special Rapporteurs published a joint Report[123] on the proposal, raising a number of human rights concerns over the definition of 'terrorist content', as well as Article 4 (on removal orders), Article 5 (on referrals for voluntary considerations) and Article 6 (on proactive measures).[124] The European Parliament approved the proposal in April 2019.[125]

Several international human rights instruments regulate extremist content, hate speech and the promotion of terrorism, as well. The International Covenant on Civil and Political Rights (ICCPR), for example, makes clear that: "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."[126] The International Convention on the Elimination of all Forms of Racial Discrimination specifically addresses hate speech, as well.[127]

Apart from what has been discussed above, and the steady flow of academic works,[128] there are also numerous non-legislative initiatives that should be noted, including:

On **23 September 2019** a group of independent **UN** experts published an open letter calling on States and social media firms to take action to curb the spread of hate speech.[129]

On **18 September 2019**, the **US** Senate Committee on Commerce, Science, and Transportation held a hearing titled 'Mass Violence, Extremism, and Digital Responsibility'.[130] At the hearing, representatives from Facebook, Google and Twitter were asked questions relating to how they address such content.

There were reports in **August 2019** that the **OECD** would support efforts by Australia and New Zealand to tackle extremist speech online with proposed measures to include requiring platforms to report on the removal of extremist content.[131]

As a reaction to the terrorist attack in Christchurch in March 2019, **New Zealand** Prime Minister, Jacinda Ardern, and **French** President, Emmanuel Macron brought together Heads of State and Government and leaders from the tech sector to adopt the Christchurch Call on **15 May 2019**.[132] Other initiatives stemming from the posting of videos of the Christchurch shootings include **Australian** telecommunications companies proactively blocking access to websites hosting the terror video in the days following the attack[133] and Amazon-owned gaming platform Twitch suing users for posting the content online.[134]

---

123. United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. (2018, December 7). *Joint Report on the European Union's proposal for a Regulation on preventing the dissemination of terrorist content online to complement Directive 2017/541 on combating terrorism.* OL OTH 71/2018. Retrieved from https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234.

124. Internet & Jurisdiction Policy Network. (2018, December). EU Council adopts negotiating position on regulation against online terrorist content, endorsing one-hour takedown upon notice and proactive measures against content reappearance. *I&J Retrospect Database.* Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7726_2018-12.

125. European Parliament. (2019, April 17). *Terrorist content online should be removed within one hour, says EP.* [Press Release]. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20190410IPR37571/terrorist-content-online-should-be-removed-within-one-hour-says-ep

126. United Nations, General Assembly. (1966). International Covenant on Civil and Political Rights. *Treaty Series*, *999*, 171, Article 20(2). In ratifying the ICCPR, some states (including the US) have, however, attached reservations to Article 20.

127. United Nations. (1966). International Convention on the Elimination of All Forms of Racial Discrimination. *Treaty Series*, *660*, 195, Article 4.

128. For example, in September 2019, the George Washington University Program on Extremism released three new papers on Online Violent Extremism. Retrieved from https://www.hsdl.org/c/three-new-papers-online-violent-extremism/.

129. United Nations. (2019, September 23). *Joint open letter on concerns about the global increase in hate speech.* Retrieved from https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25036&LangID=E.

130. US Senate Committee on Commerce, Science and Transportation. (2019, September 18). *Mass violence, extremism, and digital responsibility.* Retrieved from https://www.commerce.senate.gov/public/index.cfm/2019/9/mass-violence-extremism-and-digital-responsibility.

131. Sky News. (2019, August 26). *OECD join push to tackle online extremism.* Retrieved from https://www.skynews.com.au/details/_6076962754001.

132. *Christchurch call to eliminate terrorist and violent extremist content online.* Retrieved from https://www.christchurchcall.com/call.html.

133. C, Knaus. (2019, March 19). Australian telcos block dozens of websites hosting Christchurch terror video. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2019/mar/19/australian-telcos-block-dozens-of-websites-hosting-christchurch-terror-video.

134. Kelly, M. (2019, June 19). Twitch sues to unmask trolls that posted violent and pornographic streams. *The Verge.* Retrieved from https://www.theverge.com/2019/6/17/18682395/twitch-amazon-sues-anonymous-trolls-porn-christchurch.

The **G20** meeting in Osaka in **2019** produced a Leaders' Statement On Preventing Exploitation Of The Internet For Terrorism And Violent Extremism Conducive To Terrorism.[135]

The **Dangerous Speech Project** has published a detailed practical guide defining Dangerous Speech, explaining how to determine which messages are dangerous, and illustrating why the concept is useful for preventing violence.[136]

In **October 2018**, the **US** Department of Justice launched a new hate crimes website.[137]

In **September 2018**, **Twitter** launched a consultation seeking input on its proposed amendment to the Twitter Rules (the Rules) to address dehumanization.[138]

The work of **Global Counterterrorism Forum** includes the online environment and it has produced tools such as the **September 2018** Policy Toolkit on the Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online.[139]

In **June 2018**, the **European Court of Human Rights** issued a non-binding fact sheet regarding hate speech.[140]

On **January 3, 2018**, it was reported that the Ministry of Information and Communications Technology of **Indonesia** was launching an automated Internet moderation system to detect and restrict access to extremist and adult content, as announced in November 2017.[141] The launch of the system coincides with the creation of the Indonesian National Cyber and Encryption Agency (BSSN), which is tasked with combating extremist content and misinformation online.[142]

There are other bilateral and multilateral statements of commitments to address the criminal and extremist use of the internet, including the **French-British** Action Plan on internet Security (**2017**),[143] **Five Country** Ministerial Statement on Countering Illicit Use of Online Spaces (**2018**)[144] and G7 Security Minister's Commitment Statement (**2018**), which refers to the prevention of violent extremism and terrorist use of the internet.[145] In April **2019**, the **G7** released an Outcomes Document on Combating the Use of the Internet for Violent and Extremism purposes and called for internet companies to take more proactive measures against the uploading of terrorist and violent content.[146]

---

135. G20. (2019). *Osaka leaders' statement on preventing exploitation of the Internet for terrorism and violent extremism conducive to terrorism (VECT)*. Retrieved from https://g20.org/en/documents/final_g20_statement_on_preventing_terrorist_and_vect.html.
136. Dangerous Speech Project. Retrieved from https://dangerousspeech.org/guide/.
137. United States Department of Justice. *Hate crimes*. Retrieved from https://www.justice.gov/hatecrimes.
138. Gadde, V. & Harvey, D. (2018, September 25). Creating new policies together. *Twitter*. Retrieved from https://blog.twitter.com/official/en_us/topics/company/2018/Creating-new-policies-together.html.
139. Global Counterterrorism Forum. (2018, September). *Policy toolkit on the Zurich-London recommendations on preventing and countering violent extremism and terrorism online*. Retrieved from https://www.thegctf.org/Tools-and-Manuals/Policy-Toolkit-on-the-Zurich-London-Recommendations-on-Preventing-and-Countering-Violent-Extremism-and-Terrorism-Online.
140. European Court of Human Rights. (2018, June). *Factsheet - Hate speech*. Retrieved from https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.
141. The Straits Times. (2018, January 3). *Indonesia launches cyber agency to tackle extremism, fake news*. Retrieved from http://www.straitstimes.com/asia/se-asia/indonesia-launches-cyber-agency-to-tackle-extremism-fake-news.
142. Internet & Jurisdiction Policy Network. (2018, January). Indonesia. New cyber agency launches automated system to detect and block extremist content and adult websites. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6695_2018-01.
143. French-British Action Plan: Internet security. (2017, June 13). Paris. Retrieved from https://www.gov.uk/government/publications/french-british-action-plan-internet-security.
144. Five Country Ministerial Statement on Countering the Illicit Use of Online Spaces. (2018, August 28-29). Gold Coast. Retrieved from https://archive.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/countering-illicit-use-online-spaces.
145. G7 Security Minister's Commitment Statement. (2018). Charlevoix. Retrieved from https://g7.gc.ca/en/g7-presidency/themes/building-peaceful-secure-world/g7-ministerial-meeting/chairs-statement-security-ministers-meeting/g7-security-ministers-commitments-paper/.d
146. G7 Outcomes Document on Combating the Use of the Internet for Violent and Extremist Purposes. (2019, April). Paris. Retrieved from https://www.elysee.fr/admin/upload/default/0001/04/287b5bb9a30155452ff7762a9131301284ff6417.pdf.

In **2017**, the **Global Internet Forum to Counter Terrorism** was formed by Facebook, Microsoft, Twitter, and YouTube to formalize and structure how these companies work together to curtail the spread of terrorism and violent extremism. A key facility is the shared industry hash database through which the companies can create 'digital fingerprints' for terrorist content and share it with participating companies. The sharing network has expanded, with several additional companies joining the work.[147]

The **June 2017** Statement by the heads of the member states of the **Shanghai Cooperation Organisation** on joint counteraction to international terrorism emphasized "the need for collective measures to counteract the dissemination of the ideology of terrorism and extremism, including the prevention and curtailment of terrorist and extremist propaganda, incitement to terrorism and extremism, as well as recruitment, including recruitment via the internet."[148] This statement must be read in the context of the Shanghai Convention on Combating Terrorism, Separatism and Extremism.[149]

In **2016**, Facebook, Microsoft, Twitter, and YouTube, agreed to a Code of conduct on countering illegal hate speech online presented by the **EU Commission.** Additional parties joined the arrangement in 2019.[150]

UNESCO published a report titled Countering Online Hate Speech in **2015**.[151]

In **2015**, freedom of expression group **ARTICLE19** published a 'toolkit' providing guidance to help explain and effectively counter hate speech, while protecting the rights to freedom of expression and equality.[152] ARTICLE19 also published a particularly relevant report in **2018**.[153]

In **2015**, **Jordan** launched the Aqaba meetings which are a series of international meetings to bolster security and military cooperation, coordination and exchange of expertise among regional and international partners to counter terrorism within a holistic approach.[154]

In **2013**, the **Australian** Human Rights Commission published its Background paper: Human rights in cyberspace.[155] And on **30 June 2019**, the Australian Taskforce to combat terrorist and extreme violent material online published a Report.[156]

Following a series of expert workshops organized by the Office of the High Commissioner for Human Rights (**OHCHR**), the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence was adopted in **2012**.[157]

---

147. Google. (2017, December 4). *Update on the Global Internet Forum to Counter Terrorism*. Retrieved from https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/.
148. Shanghai Cooperation Organisation. (2017, June). *Statement by the heads of the member states of the Shanghai Cooperation Organisation on joint counteraction to international terrorism.* Retrieved from http://eng.sectsco.org/load/295671/.
149. Shanghai Cooperation Organisation. (2001, June 15). *Shanghai convention on combating terrorism, separatism and extremism*. Retrieved from https://www.refworld.org/docid/49f5d9f92.html
150. European Commission. (2019). Retrieved from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en.
151. UNESCO. (2015). *Countering online hate speech*. Retrieved from http://unesdoc.unesco.org/images/0023/002332/233231e.pdf.
152. ARTICLE19. (2015). *'Hate speech' explained: A toolkit*. Retrieved from https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf.
153. ARTICLE19. (2018). *Responding to 'hate speech' with positive measures: A case study from six EU countries.* Retrieved from https://www.article19.org/wp-content/uploads/2018/06/Responding-to-'hate-speech'-with-positive-measures-A-case-study-from-six-EU-countries-.pdf.
154. Jordan Times. (2019, February 26). *King participates in tech-focused Aqaba meetings hosted by US*. Retrieved from http://www.jordantimes.com/news/local/king-participates-tech-focused-aqaba-meetings-hosted-us.
155. Australian Human Rights Commission. (2013). *Background paper: Human rights in cyberspace.* Retrieved from https://www.humanrights.gov.au/our-work/rights-and-freedoms/publications/background-paper-human-rights-cyberspace.
156. *Report of the Australian Taskforce to combat terrorist and extreme violent material online.* (2019, June 30). Retrieved from https://www.pmc.gov.au/resource-centre/national-security/report-australian-taskforce-combat-terrorist-and-extreme-violent-material-online.
157. The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, A/HRC/22/17/Add.4, Appendix, adopted 5 October 2012.

The Council of Europe issued a General Policy Recommendation on Combating the Dissemination of Racist, Xenophobic and Anti-Semitic Material via the internet in **2000**,[158] and in **2003**, it issued an additional protocol to the Convention on Cybercrime that addresses online expression of racism and xenophobia.[159]

An initiative of the **UN** Counter-Terrorism Committee Executive Directorate, 'Tech Against Terrorism', aims to support the technology industry, including smaller technology companies, in combatting terrorist exploitation of the internet. It has launched a 'Knowledge Sharing Platform' to help smaller technology companies promote the sharing of good practices that strengthen responses in this area.[160] Note also the UN's **2016** Plan of Action to Prevent Violent Extremism.[161]

The not for profit Southern Poverty Law Center monitors and reports on hate groups and sites in the **US**.[162]

There are also various **UN** Security Council Resolutions that seek to address the use of the internet for terrorist purposes.[163]

3.1.2

Defamation

Cross-border internet defamation disputes have a relatively long history of prominence in legal discussions, dating back to the well-known case of *Dow Jones v Gutnick* in 2002 – a dispute between an Australian businessman and a US-based publisher.[164] The cost of litigation keeps the number of cross-border internet defamation disputes low,[165] and the topic now receives less attention in academic literature and policy discussions. Indeed, defamation issues were infrequently raised in interviews and survey results. Nevertheless, as noted by one interviewed expert, anecdotal evidence suggests that people are more inclined to criticize other persons, companies and views online, and may resort to lies and exaggerations in their reputational attacks. And as in many other legal fields, litigants often pursue internet intermediaries in defamation cases, adding to jurisdictional complexity. For example, on December 6, 2017, the First Chamber of the Mexican Supreme Court of Justice of the Nation confirmed that Mexican courts have jurisdiction over Google, as the internet platform's actions have implications for Mexican citizens' rights.[166] The platform had argued that the Mexican courts lacked jurisdiction over US-based Google by filing a writ of *amparo*,[167] which allows physical or moral persons to seek remedy for

158. Council of the European Union (2000). *General policy recommendation on combating the dissemination of racist, xenophobic and anti-semitic material via the internet*. Retrieved from https://rm.coe.int/ecri-general-policy-recommendation-no-6-on-combating-the-dissemination/16808b5a8d.
159. Council of the European Union. (2003, January 28). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, ETS No.189 Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.
160. United Nations, Counter-Terrorism Committee Executive Directorate. *Tech against terrorism*. Retrieved from https://www.techagainstterrorism.org.
161. United Nations. *Plan of action to prevent violent extremism*. Retrieved from https://www.un.org/counterterrorism/ctitf/en/plan-action-prevent-violent-extremism.
162. Southern Poverty Law Centre. Retrieved from https://www.splcenter.org.
163. United Nations, Counter-Terrorism Committee Executive Directorate. (2018, September 14). *Public-private efforts to address terrorist content online: A year of progress – what's next?*. Retrieved from https://www.un.org/sc/ctc/news/event/public-private-efforts-address-terrorist-content-online-year-progress-whats-next/; UN Security Resolution 2129, S/RES/2129 (2013), Un Security Council Resolution 2354, S/RES/2354 (2017), UN Security Council Resolution 2395, S/RES/2395 (2017) and UN Security Council Resolution 2396, S/RES/2396 (2017).
164. Dow Jones and Company Inc v Gutnick [2002] HCA 56.
165. There are, however, still prominent cases being litigated at the highest levels. See e.g.: Haaretz.com *v*. Goldhar, 2018 SCC 28, [2018] 2 S.C.R. 3.
166. Riquelme, R. & Galindo, J. S. (2017, December 6). La Suprema Corte confirma sentencia contra Google en Mexico. *El Economista*. Retrieved from https://www.eleconomista.com.mx/empresas/Companias-extranjeras-pueden-ser-juzgadas-en-Mexico-SCJN-20171206-0075.html.
167. Available In some Spanish-speaking legal systems, a writ of amparo is a remedy for the protection of constitutional rights. See: Wikipedia. *Recurso de Amparo*. Retrieved from https://en.wikipedia.org/wiki/Recurso_de_amparo.

the protection of rights not protected specifically, but generally enshrined, in the Constitution of Mexico. The First Chamber of the Supreme Court rejected this argument by citing the *pro persona* principle, under which the imperative to protect Mexicans' fundamental rights has priority over other jurisdictional principles. However, it did not pronounce itself on the merits of the appeal itself.[168]

Google had filed an appeal in a case heard in the Eighth Civil Court of Mexico City, where the defendant, Morales, sued Google for refusing to remove a defamatory blog hosted on Google's Blogger.com platform.[169] Following the First Chamber Supreme Court's rejection of its writ of amparo, Google Mexico indicated that it had withdrawn its appeal, therefore avoiding a Supreme Court ruling on the general jurisdictional scope of Mexican courts against Google.[170]

Apart from the type of jurisdictional issues that arose in the Mexican case, online defamation has an international dimension stemming from the fact that the right of reputation is protected in various international human rights instruments and is often seen as conflicting with the right of freedom of expression. In fact, several international human rights instruments specifically stress that freedom of expression is subject to restrictions designed to protect the reputations of others.[171]

While the overall attention directed at online defamation has decreased, new 'twists' on classical defamation issues still arise, such as the question of whether auto-completed search terms may amount to defamation – an issue that has been before the courts in Japan,[172] Australia,[173] Hong Kong SAR,[174] and Germany[175]. Issues of scale also arise, for example, when an original publication is republished through retweeting. A publication that originally only reached a small group of people may, through online republication, suddenly have a global reach and connect to a large number of countries. In such situations, the original publisher may end up exposed to a much larger legal risk than what could have reasonably been predicted. Observations of the potential reach of publications online were also made by the European Court of Human Rights in an unsuccessful application by Delfi, an Estonian online news outlet, where the Court found Delfi liable for defamatory comments posted by users on an online article.[176]

---

168. Internet & Jurisdiction Policy Network. (2017, December). Mexican Supreme Court rejects Google's argument that Mexican courts do not have jurisdiction over the platform. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6609_2017-12.

169. Garcia, D. (2017, June 15). Demandan a Google por fraude en México. *El Universal*. Retrieved from http://www.eluniversal.com.mx/articulo/nacion/sociedad/2017/06/15/demandan-google-por-fraude.

170. Reyes, J. P. (2017, December 6). Google se desiste de amparo la Suprema corte. *Excelsior*. Retrieved from http://www.excelsior.com.mx/nacional/2017/12/06/1206075. See also a somewhat similar situation in Colombia: http://www.corteconstitucional.gov.co/relatoria/autos/2018/a285-18.htm.

171. See e.g. ICCPR, Article 19(3).

172. Hornyak. T. (2013, April 16). Google loses autocomplete defamation suit in Japan. *CNet*. Retrieved from https://www.cnet.com/news/google-loses-autocomplete-defamation-suit-in-japan/.

173. Swinson, J, Lai, P. & English, J. (2018, June 13). Google this: The High Court allows Google to be sued for defamation. *King and Wood Mallesons*. Retrieved from https://www.kwm.com/en/au/knowledge/insights/trkulja-v-google-high-court-australia-appeal-20180613 and Google Inc v Duffy [2017] SASCFC 130.

174. Lau, S. (2014, August 6). Hong Kong tycoon can sue Google over 'autocomplete' search suggestions, court rules. *South China Morning Post*. Retrieved from https://www.scmp.com/news/hong-kong/article/1567521/hong-kong-court-rules-tycoon-can-sue-google-over-autocomplete-search.

175. See e.g.: Case of former German First Lady: Niggemeier, S. (2012, September 20). Autocompleting Bettina Wulff: Can a Google function be libelous? *Spiegel Online*. Retrieved from http://www.spiegel.de/international/zeitgeist/google-autocomplete-former-german-first-lady-defamation-case-a-856820.html.

176. Global Freedom of Expression, Columbia University. *Delfi AS v. Estonia*. Retrieved from https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/.

Some noteworthy developments and initiatives include:

In **August 2019**, the **Institute of International Law** published its Resolution concerning Injuries to Rights of Personality Through the Use of the Internet: Jurisdiction, Applicable Law and Recognition of Foreign Judgments.[177] The Resolution addresses a limited selection of issues that arise in civil claims arising from injuries caused through the use of the Internet to a person's rights of personality, defined to include in particular "a person's reputation, dignity, honour, name, image and privacy, as well as similar rights that, regardless of how they are called, are protected by the applicable law".[178]

During **2019**, the Defamation Working Party, established by Australia's Council of Attorneys-General, is undertaking a review of defamation law in **Australia** to identify areas for national reform.[179]

In **2018**, the Office of the Privacy Commissioner of **Canada** issued its Draft Position on Online Reputation as part of its work on 'Reputation and Privacy' – one of its strategic privacy priorities for 2015-2020.[180]

On **November 10, 2018**, it was reported[181] that Facebook had rejected the government of **Singapore**'s request to remove a post of an online article critical of the government. The country's Law Ministry reportedly pointed out that Facebook declined to take down a post that is clearly false, defamatory and uses falsehoods to attack Singapore, and has indicated that the case showed the need for regulation on misinformation online.[182]

In **October 2018**, the **Council of Europe** published its Draft study on forms of liability and jurisdictional issues in the application of civil and administrative defamation laws in Council of Europe member states.[183]

The Law Commission of **Ontario** is undertaking a major project focused on defamation law in the internet age: "The project is examining the underlying purpose and function of Ontario's defamation laws and how defamation law should be updated to account for 'internet speech,' including social media, blogs, internet platforms and digital media."[184] The project's Consultation Paper, released in **November 2017**, included a section on jurisdiction and choice of law.[185]

The **Council of Europe**'s Declaration by the Committee of Ministers on the Desirability of International Standards dealing with Forum Shopping in respect of Defamation was adopted on **July 4, 2012**.[186]

---

177. Institute of International Law. (2019, August). *Resolution concerning injuries to rights of personality through the use of the Internet: Jurisdiction, applicable law and recognition of foreign judgments.* Retrieved from http://www.idi-iil.org/app/uploads/2019/09/8-RES-EN.pdf.
178. Institute of International Law. (2019, August). *Resolution concerning injuries to rights of personality through the use of the Internet: Jurisdiction, applicable law and recognition of foreign judgments.* Retrieved from http://www.idi-iil.org/app/uploads/2019/09/8-RES-EN.pdf.
179. Council of Attorneys-General. (2019, February). *Review of model defamation provisions.* Retrieved from https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/Final-CAG-Defamation-Discussion-Paper-Feb-2019.pdf.
180. Office of the Privacy Commissioner of Canada. (2018). *Draft OPC Position on online reputation.* Retrieved from https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/.
181. Ungku, F. (2018, November 20). Singapore lawmaker blasts Facebook over refusal to take down 'false' post. *Reuters.* Retrieved from https://www.reuters.com/article/us-singapore-politics-facebook/singapore-lawmaker-blasts-facebook-over-refusal-to-take-down-false-post-idUSKCN1NP0KZ?feedType=RSS&feedName=technologyNews.
182. Internet & Jurisdiction Policy Network. (2018, November). Singapore threatens anti-misinformation regulation following Facebook refusal to take down post critical of government. *I&J Retrospect Database.* Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7682_2018-11.
183. Council of Europe. (2018, October 19). *Draft study on forms of liability and jurisdictional issues in the application of civil and administrative defamation laws in Council of Europe member states.* MSI-AUT(2018)04. Retrieved from https://rm.coe.int/draft-study-on-forms-of-liability-and-jurisdictional-issues-in-the-app/16808ef307.
184. Law Commission of Ontario. *Defamation in the internet age.* Retrieved from https://www.lco-cdo.org/en/our-current-projects/defamation-law-in-the-internet-age/.
185. Law Commission of Ontario. *Defamation in the internet age: Consultation paper.* Retrieved from http://www.lco-cdo.org/wp-content/uploads/2017/12/Defamation-Consultation-Paper-Eng.pdf, pp. 69-73.
186. Council of Europe. (2012, July 4). *Declaration by the Committee of Ministers on the Desirability of International Standards dealing with Forum Shopping in respect of Defamation.* Retrieved from https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/C10Tb8ZfKDoJ/content/declaration-of-the-committee-of-ministers-on-the-desirability-of-international-standards-dealing-with-forum-shopping-in-respect-of-defamation-libel-to?inheritRedirect=false.

3.1.2.1 Geographical scope of the right to reputation

Cross-border defamation disputes frequently give rise to 'scope of jurisdiction' issues.[187] For example, when damages are awarded for defamatory content published online, the question may arise as to whether global or more limited damages should be awarded, such as only for publications in a specific state. These issues may arise for both online[188] and offline[189] cross-border defamation.

In *Dow Jones v Gutnick*, the plaintiff limited his claim to damages suffered due to publications in Australia. But when plaintiffs seek damages for publications occurring outside the state in which the court sits, or even worldwide damages, the court must either limit the geographical scope of the damages awarded or engage in the complex exercise of assessing what is essentially 'foreign damages'. This latter option may be controversial due to its potential interference with freedom of expression in the affected state(s); i.e., a court may end up awarding damages for publications occurring in states in which the content would not be viewed as defamatory.

The problem is further amplified when plaintiffs seek deletion or rectification of the defamatory content, rather than damages. This was a central question in a 2017 decision by the Court of Justice of the European Union (CJEU).[190] In *Bolagsupplysningen OÜ*, the CJEU held that a person can bring an action for: (a) rectification of incorrect information concerning that person, (b) removal of infringing comments relating to that person, and (c) compensation in respect of all damage sustained, before the courts of the Member State in which its 'centre of interests' is located.[191]

The judgment did not make it explicitly clear whether the rectification and removal would have a global effect. On 3 October 2019, the CJEU was presented with the opportunity to clarify this controversial matter in a case referred to it by the Austrian Supreme Court.[192] The Advocate General's Opinion was published on 4 June 2019.[193] Advocate General Szpunar concluded that the EU's Directive on electronic commerce does not regulate the scope of jurisdiction question, and that it therefore does not preclude that a host provider is ordered to remove worldwide information disseminated via a social network platform.[194] The CJEU only dealt with the scope of jurisdiction matter briefly. Having embraced Advocate General Szpunar's conclusion just mentioned, it only added that: "It is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those [the rules applicable at international level]."[195]

Importantly, however, Advocate General Szpunar also emphasized that:

> "To conclude, it follows from the foregoing considerations that the court of a Member State may, in theory, adjudicate on the removal worldwide of information disseminated via the internet. However, owing to the differences between, on the one hand, national laws and, on the other, the protection of the private life and personality rights provided for in those laws, and in order to respect the widely recognised fundamental rights, such a court must, rather, adopt an approach of self-limitation. Therefore, in the interest of international comity, [...], that court should, as far as possible, limit the extraterritorial effects of its junctions concerning harm to private life and personality rights. The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. Thus, instead of removing the content, that court might, in an appropri-

---

187. For example, this issue was specifically raised in the June 2019 supplementary questions to stakeholders raised by Australia's Council of Attorneys-General Review of Model Defamation Provisions.

188. See e.g.: Cases C-509/09 eDate Advertising GmbH and Others v X and Société MGN Limited and C-161/10 Martinez and Martinez.

189. See e.g.: Case C-68/93 Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA.

190. Case C-194/16 Bolagsupplysningen OÜ Ingrid Ilsjan v Svensk Handel AB.

191. Case C-194/16 Bolagsupplysningen OÜ Ingrid Ilsjan v Svensk Handel AB, para 50. See further: Van Calster. G. *Close, but no sigar. The CJEU on libel, internet and centre of interests in Bolagsupplysningen*. Retrieved at: https://gavclaw.com/2017/11/15/close-but-no-sigar-the-cjeu-on-libel-internet-and-centre-of-interests-in-bolagsupplysningen/.

192. Case C-18/18 Glawischnig-Piesczek.

193. Opinion of Advocate General Szpunar in Glawischnig-Piesczek (Case C-18/18). The Opinion is analysed in detail in Keller. D. *Dolphins in the net: Internet content filters and the Advocate General's Glawischnig-Piesczek v. Facebook Ireland Opinion*. Retrieved at: https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-AG-Analysis.pdf, van Calster. G.,*The internet's not written in pencil, it's written in ink. Szpunar AG in Eva Glawischnig-Piesczek v Facebook, re i.a. jurisdiction and removal of hate speech. (As well as confirming my reading of his Opinion in Google)*. Retrieved from https://gavclaw.com/2019/06/07/the-internets-not-written-in-pencil-its-written-in-ink-szpunar-ag-in-eva-glawischnig-piesczek-v-facebook-re-i-a-jurisdiction-and-removal-of-hate-speech-as-well-as-confirming-my/ and in Svantesson. D. *Grading AG Szpunar's Opinion in Case C-18/18 – A caution against worldwide content blocking as default*. Retrieved at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3404385.

194. Opinion of Advocate General Szpunar in Glawischnig-Piesczek (Case C-18/18). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=174621, para 109.

195. Case C-18/18 Glawischnig-Piesczek. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1956673, para 52. See further: Smith, G. (2019, October). *Bird & Bird*. Retrieved from https://www.twobirds.com/en/news/articles/2019/global/notice-and-stay-down-orders-and-impact-on-online-platforms#__prclt=pzS67trR, and van Calster, G. (2019, October 10). Steady now. Eva Glawischnig-Piesczek v Facebook. The CJEU on jurisdiction and removal of hate speech. *GAVC Law*. Retrieved from https://gavclaw.com/tag/c-18-18/.

ate case, order that access to that information be disabled with the help of geo-blocking."[196]

On 23 October 2019, the High Court of Delhi granted an order requiring Facebook, Twitter and Google to remove certain content globally based on that content being defamatory under local law in India. In reaching its decision, the Indian Court relied on a string of recent decisions from around the world, including the CJEU's ruling in Case C-18/18. This is significant since, following the CJEU's decision in Case C-18/18, several leading commentators argued that the decision was no more than a decision about the dividing line between EU law and national law, and not a green light to global takedown orders.[197]

However, this Indian judgment highlights, with complete clarity, just how Case C-18/18 now is being used by foreign courts. This shows just how careful courts must be as to the messaging of their judgments.

The issue of scope of jurisdiction, including additional case law, is discussed in more detail in Chapter 4.1.7.

3.1.2.2 Suppression orders and contempt of court

The jurisdictional aspects of contempt orders came to prominence in the high-profile court case against Cardinal Pell for the sexual assault of two choirboys. At the time the verdict was delivered, reporting of the trial was banned under a suppression order. However, news of the verdict nevertheless spread internationally, prompting Victoria's Director of Public Prosecutions to pursue several journalists and media outlets.[198]

In essence, the issue is that suppression orders that are only enforced locally have little effect in an era where cross-border access to information is standard. At the same time, the idea the courts in one state should be allowed to dictate what journalists in other countries may report on is incompatible with most concepts of press freedom, and would set us on the course towards severely damaging freedom of expression and freedom of information.

Experts have been calling for reform to the contempt law system for some time.[199] However, there are no easy solutions, and current discussions[200] of a recognition and enforcement regime for suppression orders in foreign jurisdictions may be seen as naïve given that effectiveness requires all states to be party of such a regime.

3.1.3

Online bullying

Online bullying is predominantly a domestic matter, involving persons who have a prior relationship, such as bullying among schoolchildren. Thus, discussions of online bullying have largely taken place on a national level.[201] Yet, the cross-border dimension is obvious and unavoidable. After all, the internet platforms on which the bullying takes place are commonly based outside the jurisdiction in which the parties are located, and both access to evidence of the bullying and steps taken to have bullying content removed have clear cross-border dimensions.

Furthermore, online bullying may take place across borders, with the victim and perpetrator in different states, and may even be automated, for example, through the use of bots.

Online bullying violates the community guidelines and terms of service of virtually all major internet platforms, which also include facilities for reporting bullying content. Like the issue of non-consensual distribution of sexually explicit media discussed below, online bullying is a useful illustration of an area in which there has been extensive and fruitful collaboration among internet platforms, civil society and governments.

Defamation law is commonly applicable in situations involving online bullying, but defamation procedures are rarely pursued, largely because they are notoriously expensive. In some states, there is also a criminal law dimension to severe forms of online bul-

---

196. Opinion of Advocate General Szpunar in Glawischnig-Piesczek (Case C-18/18). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=174621, para 100.

197. Swami Ramdev & Anr. vs Facebook, Inc. & Ors. on 23 October, 2019, High Court of Delhi at New Delhi CS (OS) 27/2019. Retrieved from http://lobis.nic.in/ddir/dhc/PMS/judgement/23-10-2019/

198. Deery, S. (2019, March 26). Victorian DPP wants reporters and jailed for coverage of George Pell case. *Herald Sun*. Retrieved from https://www.heraldsun.com.au/news/law-order/victorian-dpp-wants-reporters-and-media-jailed-for-coverage-of-george-pell-case/news-story/86e42945bcdc22158738128f235b8ded.

199. Durkin, P. (2017, June 20). Outdated contempt laws need overhaul says leading law expert. *Australian Financial Review*. Retrieved from https://www.afr.com/companies/professional-services/outdated-contempt-laws-need-overhaul-says-leading-law-expert-20170620-gwup7p.

200. Victorian Law Reform Commission. *Contempt of Court Consultation Paper*. Retrieved from https://www.lawreform.vic.gov.au/projects/contempt-court-judicial-proceedings-reports-act-1958-and-enforcement-processes/contempt at pages 163-164.

201. For an insight into Colombia's experience with cyberbullying, for example, see: http://www.corteconstitucional.gov.co/relatoria/2016/T-281A-16.htm and http://www.corteconstitucional.gov.co/relatoria/2014/T-365-14.htm. The latest developments in Hong Kong are articulated in: Privacy Commissioner for Personal Data. (2019, October 8). *PCPD's Updates on Doxxing and Cyberbullying*. [Press Release]. Hong Kong. Retrieved from https://www.pcpd.org.hk/english/news_events/media_statements/press_20191008.html.

lying. Ultimately, however, active engagement from the platforms appears to be a more fruitful tool to address online bullying overall.

Finally, much like the non-consensual distribution of sexually explicit content, online bullying – especially among younger persons – is predominantly a concern in industrialized countries, as the percentage of schoolchildren with access to information technology is still low in developing countries. This will obviously change with the increasing availability of information technology in developing countries.

3.1.4

Non-consensual distribution of sexually explicit media

The non-consensual distribution of sexually explicit videos and images of an individual – sometimes referred to as 'revenge porn' – has been specifically criminalized in some states,[202] but may also be attacked under defamation law, data privacy law, breach of confidentiality or even copyright law. In cases where the perpetrator uses one of the major online platforms, instances of non-consensual distribution of sexually explicit media are – similar to online bullying – usually addressed most effectively via reporting facilities on the platform in question. This is because the non-consensual distribution of sexually explicit media violates the community guidelines and terms of service of virtually all major internet platforms.

An important trend here is that private sector platforms, rather than lawmakers, have largely taken the initiative in tackling the non-consensual distribution of sexually explicit videos and images, and in quickly establishing common norms that have only afterwards found a translation into some legal frameworks. This is an illustration of the meta-trend of norm setting by companies, discussed in Chapters 2.4.2 and 2.5.

Some platforms use photo-matching technologies to prevent the non-consensual posting or re-posting of sexually explicit media.[203] A controversial aspect of this system is that these photo-matching technologies require access to the sexually explicit media content that was distributed without consent the first place. Therefore, a person fearful of becoming a victim of non-consensual distribution of sexually explicit media will need to share the content with the platform for the photo-matching technologies to work. To prevent re-posting, however, the photo-matching technologies can of course rely on the initially detected sexually explicit content.

But the non-consensual distribution of sexually explicit media may also be carried out through other channels, such as smaller platforms or by MMS. In such instances, the safeguards discussed above are not necessarily available.

The non-consensual distribution of sexually explicit media should not be confused with the forms of 'sexting' that involve the voluntary sharing of sexually explicit videos and images. Yet, such voluntary sharing may still give rise to complex legal issues, such as instances when an underage person voluntarily shares sexually explicit video and images. Initially, sexually explicit media is often shared voluntarily, but later distributed without consent. This highlights a link between voluntary sexting and the non-consensual distribution of sexually explicit media. There are some initiatives worth noting, including:

- **Australia**'s Online Safety (Non-Consensual Sharing of Intimate Images) Act **2018** provides penalties for those who post, or threaten to post, intimate images of others online without their consent. It is an offence for perpetrators, websites, social media providers and content hosts to fail to remove offending content upon request by the eSafety Commissioner.[204] The eSafety Commissioner has a number of initiatives including an image-based abuse portal and a safety by design initiative.[205]
- In the area of child sexual abuse content, the **Child Dignity Alliance Technical Working Group** report of **2018** provides technical recommendations to both government and industry including the establishment of a technical inventory of tools and technologies to assist law enforcement.[206]
- The **Internet Watch Foundation** works to identify and remove child sexual abuse content online and provides an international reporting portal.[207]
- **5Rights Foundation** advocates for the rights to children in the digital world.[208]

---

202. For example, one surveyed expert referred to Article 71 bis of the City Contravention Code of Buenos Aires, Argentina which specially refers to unauthorized spread of intimate photos and videos on the internet ("any kind of electronic communication mean"), as well as Article 493 of the National Draft Bill of the Criminal Code, Argentina. Retrieved from http://www.pensamientopenal.com.ar/system/files/2018/06/legislacion46694.pdf.

203. See e.g.: Davis, A. (2017, April 5). Using technology to protect intimate images and help build a safe community. *Facebook newsroom*. Retrieved from https://newsroom.fb.com/news/2017/04/using-technology-to-protect-intimate-images-and-help-build-a-safe-community/.

204. Timebase. (2018, September 13). *Criminalising the non-consensual online sharing of intimate images*. Retrieved from https://www.timebase.com.au/news/2018/AT04790-article.html.

205. Australian eSafety Commissioner. Retrieved from https://www.esafety.gov.au/.

206. Child Dignity Alliance. (2018, November). *Child Dignity Alliance Technical Working Group Report*. Retrieved from https://www.childdignity.com/technical-working-group-report.

207. Internet Watch Foundation. Retrieved from https://www.iwf.org.uk.

208. 5Rights Foundation. Retrieved from https://5rightsfoundation.com.

3.1.5

Fake News and misinformation

Neither misinformation nor cross-border misinformation are new phenomena. In recent years, however, there has been an unprecedented interest in online misinformation activities, and particularly in what has been termed 'fake news'. In its Freedom on the Net 2017 report, Freedom House observed:

> "Governments around the world have dramatically increased their efforts to manipulate information on social media over the past year. The Chinese and Russian regimes pioneered the use of surreptitious methods to distort online discussions and suppress dissent more than a decade ago, but the practice has since gone global. Such state-led interventions present a major threat to the notion of the internet as a liberating technology."[209]

The picture painted in the Freedom on the Net 2018 report suggests that these concerns remain strong.[210] Further, a 2018 study by the Reuters Institute for the Study of Journalism, based on data covering nearly 40 countries and five continents, highlighted that consumer trust in news is low in most countries, and that there are high levels of concern about fake news. This concern, the report notes, is "partly stoked by politicians, who in some countries are already using this as an opportunity to clamp down on media freedom".[211] The same study drew attention to the fact that after years of continuous growth, the use of social media for accessing news has declined in countries such as the US, the UK and France, while there is an increase in the use of messaging apps for news. This is an important trend, as it makes the policing of social media less efficient.

There are several noteworthy initiatives – from both industrialized and developing countries – seeking to address fake news and misinformation. Focusing on those outside the national defense sphere, some key initiatives are:

Social media platforms announced in **August 2019** that they identified and removed accounts linked to a "coordinated state-backed operation" by China spreading disinformation to target unrest in **Hong Kong**.[212]

The **Philippines**' proposed Anti-False Content Bill was introduced into the Senate on **July 1, 2019**. The proposed law permits the Cybercrime Office in the Justice Department to direct internet intermediaries, platforms and individuals wherever they are located to correct, take down or block access to content that is determined by the office to be false or misleading.[213]

In **May 2019**, **Singapore** passed the Protection from Online Falsehoods and Manipulation Bill which permits the government to require 'corrections' to be made to 'false' content.[214]

The **UK** Digital, Culture, Media and Sport Select Committee released a report on Disinformation and Fake News in **February 2019**[215] and an Online Harms White Paper in **April 2019**[216] with both reports calling for more regulation of platforms.

---

209. Freedom House. (2017). *Freedom on the net 2017: Manipulating social media to undermine democracy*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2017.
210. Freedom House. (2018). *Freedom on the net 2018: The rise of digital authoritarianism*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
211. Reuters Institute for the Study of Journalism. (2018). *Reuters Institute Digital News Report 2018*. Retrieved from http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475, p. 9.
212. Twitter Safety. (2019, August 19). *Information operations directed at Hong Kong*. Retrieved from https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html.
213. Human Rights Watch. (2019, July 25). *Philippines: Reject sweeping 'Fake News' Bill*. Retrieved from https://www.hrw.org/news/2019/07/25/philippines-reject-sweeping-fake-news-bill.
214. Russell, J. (2019, May 9). Singapore passes controversial 'fake news' law which critics fear will stifle free speech. *Tech Crunch*. Retrieved from https://techcrunch.com/2019/05/09/singapore-fake-news-law/.
215. UK Digital, Culture, Media and Sport Select Committee. (2019, February). *Disinformation and fake news: final report*. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.
216. UK Digital, Culture, Media and Sport Select Committee. (2019, April). *Online Harms White Paper*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf. For a discussion, see e.g.: Smith, D. (2019, May 5). The rule of law and the Online Harms White Paper. *Cyberleagle*. Retrieved from https://www.cyberleagle.com/2019/05/the-rule-of-law-and-online-harms-white.html.

In **2018**, members of the **International Grand Committee**, including members of the national parliaments of Argentina, Belgium, Brazil, Canada, France, Latvia, Singapore and the UK signed the declaration on Principles of the Law Governing the Internet, addressing 'fake news' and disinformation online.[217]

On **December 7, 2018**, it was reported[218] that officials from **India**'s Ministry of Electronics and Information Technology had met with Facebook representatives to trace the origins of misinformation that spread through Facebook-owned messaging platform WhatsApp and led to violent outbursts.[219]

On **October 26, 2018**, Facebook announced that it had removed 82 pages, groups and accounts that were linked to **Iran** and spread misinformation on Facebook and Instagram. These accounts were followed by more than 1 million users:[220] "The Page administrators and account owners typically represented themselves as US citizens, or in a few cases UK citizens – and they posted about politically charged topics such as race relations, opposition to the President, and immigration."[221]

In **2018**, **Malaysia** introduced its Anti-Fake News Act. An attempt to repeal the controversial law was rejected in **September 2018**.[222]

In **July 2018**, it was reported[223] that members of **Russia**'s governing party, United Russia, had submitted a bill that proposes holding social networks accountable for 'inaccurate' comments that users post. In particular, the law would reportedly require websites with over 100 000 daily visitors to take down factually inaccurate posts or face fines of up to 50 million rubles (about 800 000 US dollars).[224] In **March 2019** there were reports that Russia's president signed a new law criminalizing users who spread what the government deems to be misinformation, including content that shows "blatant disrespect" for the government.[225]

On **May 9, 2018**, **The Gambia**'s Supreme Court ruled that the prohibition of 'false publication and broadcasting' was constitutional, upholding the illegality of spreading false news online, which was introduced as part of the Information and Communications Act 2013.[226] On May 10, 2018, The Gambia's Press Union Secretary General Saikou Jameh stated that the ruling was a striking departure from a recent ruling by the Economic Community of West African States (ECOWAS) court, which had ruled that the rules violated the rights of journalists and called on the Gambian government to immediately repeal them.[227]

---

217. UK Commons Select Committee. (2018, November 27). *Parliamentarians from across the world sign declaration on the 'Principles of the Law Governing the Internet'*. Retrieved from https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/declaration-internet-17-19/.

218. Phartiyal, S. (2018, December 7). India government meets with WhatsApp over tracing of fake news: source. *Reuters*. Retrieved from https://www.reuters.com/article/us-india-whatsapp-government/india-government-meets-with-whatsapp-over-tracing-of-fake-news-source-idUSKBN1O60GO?feedType=RSS&feedName=technologyNews.

219. Internet & Jurisdiction Policy Network. (2018, December). Indian government officials meet with WhatsApp representatives over traceability of misinformation leading to violence. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7734_2018-12.

220. Internet & Jurisdiction Policy Network. (2018, October). Facebook announces removal of pages and accounts for breaking rules against coordinated inauthentic behaviour, including some linked to Iran. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7558_2018-10.

221. Gleicher, N. (2018, October 26). Taking down coordinated inauthentic behavior from Iran. *Facebook Newsroom*. Retrieved from https://newsroom.fb.com/news/2018/10/coordinated-inauthentic-behavior-takedown/.

222. Sipalan, J. (2018, September 12). Malaysia opposition blocks repeal of 'fake news' law in challenge to Mahathir. *Reuters*. Retrieved from https://www.reuters.com/article/us-malaysia-politics-fakenews/malaysia-opposition-blocks-repeal-of-fake-news-law-in-challenge-to-mahathir-idUSKCN1LS0WO.

223. Pigman, L. (2018, July 22). Russia, Accused of faking news, unfurls its own 'fake news' Bill. *The New York Times*. Retrieved from https://www.nytimes.com/2018/07/22/world/europe/russia-fake-news-law.html.

224. Internet & Jurisdiction Policy Network. (2018, July). Russia: Proposed Bill would require platforms to remove 'factually inaccurate posts'. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7180_2018-07,

225. Baker, S. (2019, March). Vladimir Putin signed a restrictive new law that makes it illegal to insult government officials. *Business* Insider. Retrieved from https://www.businessinsider.com/vladimir-putin-law-illegal-insult-him-government-2019-3?IR=T.

226. Committee to Protect Journalists. (2018, May 10). *Gambia declares criminal defamation unconstitutional, keeps some laws on sedition, fake news*. Retrieved from https://cpj.org/2018/05/gambia-declares-criminal-defamation-unconstitution.php**.**

227. Internet & Jurisdiction Policy Network. (2018, May). Gambia Supreme Court upholds prohibition of spreading misinformation online, in spite of recent ECOWAS Court ruling. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7044_2018-05.

In **2018,** the **International Federation of Library Associations and Institutions** (IFLA) issued a statement on fake news, highlighting that disproportionate policy responses can have a big impact on intellectual freedom. The statement emphasized the importance of addressing the phenomenon through literacy and research efforts.[228]

In **2018**, **Freedom House** published its Internet Freedom: Election Monitor.[229]

The Belfer Center for Science and International Affairs, Harvard Kennedy School published an analysis of how **Sweden** protected its **2018** elections.[230]

In **2018**, the **European Union** developed, and several major internet companies signed up to, a Code of Practice on Disinformation.[231] The signatories commit "to deploy policies and processes to disrupt advertising and monetization incentives for relevant behaviours, such as misrepresenting material information about oneself or the purpose of one's properties."[232] In 2019 the EU Commission released an implementation report on the Code of Practice[233] and later issued a statement[234] calling on social media platforms to do more to reduce the spread of disinformation. Consider also the final report of the EU Commission's High Level Expert Group on Fake News and Online Disinformation.[235]

Egypt introduced a new law in **2018** that, among other things, tackles 'fake news'. Article 7 of the Anti-Cyber and Information Technology Crimes Law gives the competent authority in charge of investigating cybercrime "the right to shut down websites that spread 'fake news' against the Egyptian state or threaten 'national security'."[236] The law has an extraterritorial effect, insofar as it authorizes the competent authority "to shut down (not block) foreign websites, though it is unclear how this would happen in practice."[237]

Canada's Digital Citizen Initiative is a multi-component strategy aimed at building citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem.[238]

Through its Computational Propaganda Research Project, the **Oxford Internet Institute** has been investigating the use of algorithms, automation and computational propaganda in public life since **2012**.[239] They have published numerous reports.

---

228. International Federation of Library Associations and Institutions. (2018). *IFLA statement on fake news*. Retrieved from https://www.ifla.org/publications/node/67341.
229. Freedom House. (2018). *Internet freedom: Election monitor*. Retrieved from https://freedomhouse.org/report/special-reports/internet-freedom-election-monitor.
230. Cederberg, G. (2018, September 7). Catching Swedish phish: How Sweden is protecting its 2018 elections. *Belfer Centre for Science and International Affairs*. Retrieved from https://www.belfercenter.org/publication/catching-swedish-phish-how-sweden-protecting-its-2018-elections.
231. European Union. (2018, September 26). *Code of Practice on Disinformation*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.
232. European Union. (2018, September 26). *Code of Practice on Disinformation*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation, p. 4.
233. European Commission. (2019, February 28). *First monthly intermediate results of the EU Code of Practice against disinformation*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation
234. European Commission. (2019, May). *Code of Practice against disinformation: Commission recognises platforms' efforts ahead of the European elections*. Retrieved from https://europa.eu/rapid/press-release_MEX-19-2613_en.htm.
235. European Commission. (2018, March 12). *Final Report of the High Level Expert Group on Fake News and Online Disinformation*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
236. Internet Society. (2018, September). *The internet and extra-territorial application of laws*. Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf, p. 24.
237. Internet Society. (2018, September). *The internet and extra-territorial application of laws*. Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf, p. 24.
238. Government of Canada. *Online disinformation*. Retrieved from https://www.canada.ca/en/canadian-heritage/services/online-disinformation,html. Note also: Government of Canada's Diversity of Content initiative, see: Government of Canada. *Diversity of content in the digital age*. Retrieved from https://www.canada.ca/en/canadianheritage/services/diversity-contentdigital-age.html. One interviewed stakeholder emphasized the impact of disinformation on citizens and on social cohesion.
239. Oxford Internet Institute. *The Computational Propaganda Project*. Retrieved from https://comprop.oii.ox.ac.uk/about-the-project/.

Some interviewed experts expressed greater concerns about so-called 'deep fakes' than about 'fake news' *per se*, particularly in the context of current affairs and international politics. Deep fakes involve the technological manipulation of video and audio content, resulting in highly realistic and difficult-to-detect visual depictions and/or audio recordings of real people doing or saying things they never said or did.[240]

3.1.5.1 Attacks on democracy

Attempts to use fake news to affect election results have gained considerable attention in the context of the US presidential election in 2016, the UK Brexit vote and several other recent elections in France, Germany, Sweden and Brazil.[241] A common theme here is that fake news and misinformation campaigns are orchestrated, and in large parts operated, from outside the affected country, thus giving rise to complex jurisdictional challenges. The concern is such that repeated calls have been made against the use of e-voting systems.[242]

To date, these activities have rarely resulted in prosecutions, though charges have been made in some cases.[243] The difficulties associated with bringing foreign offenders to justice are well known. Furthermore, in cases where misinformation campaigns are carried out, supported or sanctioned by a foreign government, cross-border enforcement assistance against the offenders is particularly unlikely.

There are several reports investigating Russian interference in the 2016 US presidential election. One recent report, produced upon a request from the US Senate Select Committee on Intelligence (SSCI), focused on the activities by Russia's Internet Research Agency (IRA). The report reviewed an expansive data set of social media posts and metadata provided to the SSCI by Facebook, Twitter and Alphabet, as well as a set of related data from additional platforms.[244]

That report concluded that active and ongoing interference operations remain on several platforms.[245] It also noted that, as media covered their Facebook and Twitter operations, the IRA shifted much of its activity to Instagram, and that "Instagram is likely to be a key battleground on an ongoing basis".[246] The report showed that the "IRA had a very clear bias for then-candidate Trump that spanned from early in the campaign and throughout the data set",[247] and concluded that "we must promote a multi-stakeholder model in which researchers, tech platforms, and government work together to detect foreign influence operations that attempt to undercut public discourse and democracy."[248] A contemporaneous report by the Computational Propaganda Research Project of the Oxford Internet Institute reached similar conclusions.[249] There is, of course, also the Report on the Investigation into Russian Interference in the 2016 Presidential Election by Special Counsel Robert S. Mueller.[250]

During the Brazilian 2018 presidential election, there were multiple reports of misinformation spreading via WhatsApp, aswell as other social media platforms. On October 19, 2018,

---

240. See further: Pfefferkorn. R, (2019, September). Too good to be true? "Deep fakes" pose a new challenge for trial courts. *NWLawyer*. Retrieved from http://nwlawyer.wsba.org/nwlawyer/sept_2019/MobilePagedReplica.action?pm=2&folio=22; Browne, R. (2018, December 7). Anti-election meddling group makes A.I. powered Trump impersonator to warn about 'deep fakes'. *CNBC*. Retrieved from https://www.cnbc.com/2018/12/07/deepfake-ai-trump-impersonator-highlights-election-fake-news-threat.html; Bloomberg. (2018, September 11). How faking videos became easy: and why that's so scary. *Fortune*. Retrieved from http://fortune.com/2018/09/11/deep-fakes-obama-video/; Alliance of Democracies. *The Campaign for Democracy*. Retrieved from http://www.allianceofdemocracies.org/initiatives/the-campaign/; and Council on Foreign Relations. (2018, October 16). *Disinformation on Steroids*. Retrieved from https://www.cfr.org/report/deep-fake-disinformation-steroids.

241. But also others, such as Australia: Packham, C. (2019, September 16). Exclusive: Australia concluded China was behind hack on parliament, political parties – sources. *Reuters*. Retrieved from https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF. More generally see: Bisen, A. (2019. April 24). Disinformation is drowning democracy. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2019/04/24/disinformation-is-drowning-democracy/.

242. One surveyed expert pointed to such calls in Germany, France, Belgium, the Netherlands, Paraguay, Argentina and Peru.

243. United States of America v Netyksho et al (Case 1:18-cr-00215-ABJ). Retrieved from https://www.justice.gov/file/1080281/download.

244. New Knowledge. *The tactics and tropes of the Internet Research Agency*. Retrieved from https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, p. 3.

245. New Knowledge. *The tactics and tropes of the Internet Research Agency*. Retrieved from https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, p. 7.

246. New Knowledge. *The tactics and tropes of the Internet Research Agency*. Retrieved from https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, p. 8.

247. New Knowledge. *The tactics and tropes of the Internet Research Agency*. Retrieved from https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, p. 9.

248. New Knowledge. *The tactics and tropes of the Internet Research Agency*. Retrieved from https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, p. 100-101.

249. Oxford Internet Institute. Computational Propaganda Research Project. *The IRA, social media and political polarization in the United States, 2012-2018*. Retrieved from https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf.

250. Mueller, R.S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Retrieved from https://www.justice.gov/storage/report.pdf.

Facebook's WhatsApp announced[251] that it was taking legal action to stop companies from spreading misinformation on its platform in the context of the Brazilian presidential election. The second round of this election took place on October 28, 2018.[252]

Misinformation campaigns that aim to affect various election outcomes[253] have been a focal point in discussions about fake news and misinformation. This is a particularly important issue, as many people today use online sources to inform themselves of political issues. A June 2018 study by Internetstiftelsen i Sverige, for example, found that 71% of the study participants accessed political information on the internet in 2018, compared to just 47% in 2014.[254] While these figures will vary from country to country, there is an increasing reliance on political internet content in many countries.

3.1.5.2 Expression and platform moderation: responsibility, liability and question of neutrality

The role of internet platforms is a central topic in relation to many of the topics covered in this Report, as well as several overarching meta-trends discussed in Chapter 2. The role of these platforms has gained particularly strong attention in recent discussions about fake news and misinformation. In the aftermath of the Cambridge Analytica scandal, for example, the pressure on internet platforms increased considerably, and various legislative initiatives have been debated.

Some countries have already implemented criminal offenses that may be of relevance. Canadian law, for example, contains the following criminal offense: "Everyone who willfully publishes a statement, tale or news that he knows is false and that causes or is likely to cause injury or mischief to a public interest is guilty of an indictable offense and liable to imprisonment for a term not exceeding two years."[255] Yet the difficulty of applying content-focused law is well known and clearly illustrated in case law such as in *R. v. Zundel*,[256] where the Supreme Court of Canada was tasked with examining the constitutionality of the mentioned Section.

Striking the right balance in the context of internet platforms is difficult. On the one hand, they play an important role in censoring and countering fake news and misinformation. On the other hand, there is an obvious reluctance to make platforms act as arbiters of 'truth'. Related to the question of platform responsibility, is the question of liability versus content moderation. These issues are recurring themes throughout this Report.

Countering fake news through crowdsourcing is another alternative. POLITICO has launched one such initiative.[257] Through a combination of crowdsourced information and its own investigations, POLITICO attempts to identify potential pieces of disinformation. Once identified, the information is vetted by their staff, and if it fits their parameters for fake news, it will be reported in their findings. Users can then turn to their database to check whether items they have read online are real or fake.

---

251. Spring, J. & Brito, R. (2018, October 20). Brazil election battle rages over Facebook's WhatsApp. *Reuters.* Retrieved from https://www.reuters.com/article/us-brazil-election-facebook/brazil-election-battle-rages-over-facebooks-whatsapp-idUSKCN1MT2WP?feedType=RSS&feedName=technologyNews.

252. Internet & Jurisdiction Policy Network. (2018, October). WhatsApp announced legal action against companies spreading misinformation ahead of Brazilian elections. *I&J Retrospect Database.* Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7550_2018-10.

253. See e.g.: Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2019, June). *Research paper 1/2019: Freedom of expression and elections in the digital age.* Retrieved from https://www.ohchr.org/Documents/Issues/Opinion/ElectionsReportDigitalAge.pdf.

254. Internetstiftelsen i Sverige. (2018). *Svenskarna och internet valspecial 2018.* Retrieved from https://www.iis.se/docs/Svenskarna_och_internet-_valspecial_2018.pdf, p. 9.

255. Criminal Code (R.S.C., 1985, c. C-46), section 181.

256. R v Zundel [1992] 2 S.C.R. 731.

257. Lima, C. & Briz, A. (2018, October 7). Is this true? A fake news database. *Politico.* Retrieved from https://www.politico.com/interactives/2018/is-this-true/about/.

3.1.6

Data privacy

While data privacy has clear economic and security aspects, it is predominantly addressed here in the context of expression.

Interest in data privacy (or data protection) has increased markedly over the past 10 years, with few other topics gaining as much attention in 2018. This was strongly driven by the EU's long-awaited GDPR,[258] which came into effect on May 25, 2018. Yet, there remains much work to be done, as hinted at by the 2019 Ranking Digital Rights Corporate Accountability Index's finding that most companies still fail to disclose important aspects of how they handle and secure personal data.[259]

With the world largely preoccupied by data privacy developments in Europe, important developments elsewhere in the world – in both industrialized and developing countries – have largely been overlooked. A study highlighted that, as of January 31, 2017, no fewer than 120 countries have data privacy laws that meet minimum international standards.[260] The same study pointed to official bills for new data privacy acts (whether or not introduced into legislatures) from 30 additional countries.

Some noteworthy data privacy developments include:
On **3 July 2019**, it was reported that **Rwanda** is working on a Personal Data Protection Law.[261]
Following the receipt of privacy complaints, the **UK** Information Commissioner's Office issued a report in **June 2019** which considers the implications under the GDPR for the use of real time bidding used in advertising technology.[262]
In **February 2019**, the Personal Data Protection Commission **Singapore** published a Discussion Paper on Data Portability.[263]
In **February 2019** the **Nigerian** National Information Technology Development Agency released its draft Data Protection Regulation, inspired by the GDPR.[264]
In **2019,** the **Canadian** government released a Digital Charter: Trust in a Digital World seeking to engender trust in data protection.[265]
In **2019** and after some delays, **Finland's** Data Protection Act entered into force, implementing the GDPR.[266]

258. 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. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

259. Ranking Digital Rights. (2019). *2019 Ranking Digital Rights Corporate Accountability Index*. Retrieved from https://rankingdigitalrights.org/index2019/.

260. Greenleaf, G. (2017, January 31). Global tables of data privacy laws and bills (5th Ed 2017). *Privacy Laws & Business International Report* 145, 14-26. Retrieved from: https://ssrn.com/abstract=2992986. See also: United Nations Conference on Trade and Development. *Data Protection and Privacy Legislation Worldwide*. Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

261. Sabiiti, D. (2019, July 3). Rwanda working on a Personal Data Protection Law. *KT Press*. Retrieved from https://ktpress.rw/2019/07/rwanda-working-on-a-personal-data-protection-law/.

262. UK Information Commissioner. (2019, June 20). *Update Report into AdTech and Real Time Bidding*. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

263. Personal Data Protection Commission Singapore. (2019, February). *Discussion paper: Data portability*. Retrieved from https://www.pdpc.gov.sg/Resources/Data-Portability.

264. Internet & Jurisdiction Policy Network. (2019, February). Nigerian agency releases draft Data Protection Regulation. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoibmlnZXJpYSIsImZyb20iOilyMDE5LTAxIiwidG8iOilyMDE5LTA4In0=.

265. Innovation, Science and Economic Development Canada. (2019). *Canada's Digital Charter: Trust in a digital world*. Retrieved from https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

266. Blaszcyk, W.N. (2019, January 3). Finland: Data Protection Act enters into force after being "significantly delayed". *Data Guidance*. Retrieved from https://www.dataguidance.com/finland-new-data-protection-act-enters-into-force-after-being-significantly-delayed/.

Through Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) adopted in **2018**, the **Council of Europe** modernized its Convention 108.

In **September 2018**, the Argentinian data protection authority announced the introduction of a draft data protection bill to reform the current regime.[267] **Argentina**'s Personal Data Protection Act dates back to **2000**. However, the new data protection bill aims to bring Argentinian data protection law in line with the GDPR.

A **September 2018** amendment saw **Thailand**'s Draft Personal Data Protection Act incorporate several provisions that largely mirror approaches found in the GDPR. For example, this applies to how the matter of extraterritoriality is addressed.

In **Brazil**, the draft General Data Privacy Law was approved by the Senate and sent to the President. On **August 15, 2018**, Brazil's President Michel Temer signed into law the General Data Protection Law (*Lei Geral de Proteção de Dados*, LGPD), which establishes, for the first time in the country's history, a general framework for data protection. The law has been described as being inspired by the EU's GDPR.[268]

The **Kenyan** government is in the process of developing a Policy and Regulatory Framework for Privacy and Data Protection, including the Data Protection Bill 2018. On **July 3, 2018**, a draft bill to establish a data protection regime was introduced in the Kenyan Parliament. The bill would require individuals and companies collecting, processing and storing personal data to obtain consent from data subjects, impose data security obligations and restrictions on third-party data transfers, and introduce penalties for violations.[269]

In 2018, a bill substantially amending the Data Protection Act No. 19,628 was reviewed and processed in the Senate in **Chile**. On **June 16, 2018**, the National Congress of Chile approved a law making the 'protection of one's personal data' a constitutional right.[270] Chile joins Mexico, Colombia and Ecuador in a group of Latin American countries where the protection of data is a constitutional right.[271]

In **2018**, Privacy Bill 34-1 (2018) reforming **New Zealand**'s data privacy law was making its way through the legislative process.

The **California** Consumer Privacy Act was signed into law in **2018** and will come into effect at the beginning of **2020**. The Act regulates the conduct of businesses and extends certain rights to consumers. The Act focuses on whether the business in question "does business in the State of California".[272]

In the **United States**, the Internet Association - a trade association that exclusively represents leading global internet companies on matters of public policy - launched a campaign for a federal data privacy law.[273] A surveyed expert pointed to how critics of the campaign suggest that it could be seen as an effort to pre-empt state-based efforts similar to the California Consumer Privacy Act.[274]

---

267. Internet & Jurisdiction Policy Network. (2018, September). Argentina's draft Data Protection Bill introduced in parliament. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7465_2018-09.
268. Internet & Jurisdiction Policy Network. (2018, August). Brazil: President signs Data Protection Bill into law. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7246_2018-08.
269. Internet & Jurisdiction Policy Network. (2018, July). Kenya: Data Protection Bill introduced in Parliament. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7190_2018-07.
270. Hunton Andrews Kurth. (2018, June 28). Protection of personal data now a constitutional right in Chile. *Privacy and Information Security Law Blog*. Retrieved from https://www.huntonprivacyblog.com/2018/06/28/protection-personal-data-now-constitutional-right-chile/.
271. Internet & Jurisdiction Policy Network. (2018, June). Chile passes amendment making data protection a constitutional right. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7071_2018-06.
272. California Consumer Privacy Act of 2018, 1798.140. C(1)(a).
273. Internet Association. *Policy position: Privacy*. Retrieved from https://internetassociation.org/positions/privacy/.
274. See also: Tsukayama, H. (2019, September 4). Lawmakers Must Not Listen to the Internet Association and Weaken the California Consumer Privacy Act. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2019/09/lawmakers-must-not-let-internet-association-weaken-california-consumer-privacy-act.

In **2018**, the **Australian** Privacy Act 1988 (Cth) was amended to incorporate a mandatory data breach notification scheme. In **2019** Australia passed a Consumer Rights Bill which provides users with rights to obtain access and port their consumer data held by businesses.[275]

Following ratification of the **Council of Europe**'s Convention 108, the **Tunisian** government introduced a draft law on personal data protection in **2018** (Draft Law 25/2018).

In **India**, the Supreme Court upheld the right to privacy as a constitutionally protected value in a historic **2017** decision,[276] and in **2018**, a draft data protection bill called the Personal Data Protection Bill was presented.[277]

In **2017**, the Amended Act on the Protection of Personal Information (APPI) in **Japan** came into effect. The Act shares some similarities with the GDPR, including provisions with extraterritorial application and a new cross-border data transfer framework.

Qatar enacted its Law No. 13 Concerning Personal Data Protection (DPL) in **2016**.

The **Association of Southeast Asian Nations** (ASEAN) Framework on Personal Data Protection was established in **2016** to guide member states on data protection regulation.

In **2016**, **United Nations Conference on Trade and Development** published its report titled Data protection regulations and international data flows: Implications for trade and development.[278]

The **European Commission** has advanced a proposal for a Regulation on Privacy and Electronic Communications that will replace the ePrivacy Directive.[279]

In **2015**, the **UN Human Rights Council** appointed its first Special Rapporteur on the right to privacy. The work of the Special Rapporteur is ongoing.[280] Note also, the **2014** Report of the Office of the United Nations High Commissioner for Human Rights titled The Right to Privacy in the Digital Age.[281]

The **Global Network Initiative**'s Principles on Freedom of Expression and Privacy[282] (first launched in 2008) was updated in **2015**, and the updated Guidelines were approved in **2017**.[283]

---

275. Internet & Jurisdiction Policy Network. (2019, August). Australia passes Consumer Data Rights Bill. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiY29uc3VtZXIgZGF0YSIsImZyb20iOiIyMDEyLTAyIiwidG8iOiIyMDE5LTA4In0=.
276. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors, Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India. Aug 24, 2017).
277. PRS Legislative Research. *Draft Personal Data Protection Bill, 2018*. Retrieved from https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018.
278. United Nations Conference on Trade and Development. (2016). *Data protection regulations and international data flows: Implications for trade and development*. Retrieved from https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
279. European Commission. *Proposal for an ePrivacy regulation*. Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation. A discussion of the relationship between the GDPR and the current ePrivacy Directive can be found here: European Data Protection Board. (2019, March 12). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/stanovisko-vyboru-cl-64/opinion-52019-interplay-between-eprivacy_en.
280. See e.g.: United Nations Special Rapporteur on the Right to Privacy. (2019). *Report of the Special Rapporteur on the Right to Privacy to Human Rights Council.* A/HRC/40/63. Retrieved from https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_HRC_40_63, DOCX; United Nations Special Rapporteur on the Right to Privacy Task Force on Health Data. (2019). *Draft recommendation on the protection and use of health-related data.* Retrieved from https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf.
281. Office of the United Nations High Commissioner for Human Rights. (2014). *Report of the High Commissioner for Human Rights on the right to privacy in the digital age.* A/HRC/27/37. Retrieved from https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc.
282. Global Network Initiative. *The GNI Principles*. Retrieved from https://globalnetworkinitiative.org/gni-principles/.
283. Global Network Initiative. (2017, March 20). *GNI publishes updates to the core commitments of our membership*. Retrieved from https://globalnetworkinitiative.org/gni-publishes-updates-to-the-core-commitments-of-our-membership/.

In **2015**, the **International Federation of Library Associations and Institutions** (IFLA) issued a statement on privacy in the library environment.[284]

In **2013**, the **Organisation for Economic Co-operation and Development** (OECD) published a revised version of its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The revision emphasizes the need to address the global dimension of privacy through improved interoperability.

In **2013**, the **International Law Association** established a Committee on the Protection of Privacy in Private International and Procedural Law. The work of the Committee is ongoing.

The Center for Democracy and Technology has put forward a discussion draft on baseline privacy legislation for the **US**.[285]

Interviewed and surveyed experts emphasized the importance of coordination efforts at the international and regional level to discuss data protection issues through, for example:

- International Conference on Data Protection and Privacy Commissioners;[286]
- Asia Pacific Privacy Authorities (APPA) Forum;[287]
- Ibero-American Data Protection Network (*Red Iberoamericana*) (RIPD or RedIPD);[288]
- Latin American Network of Surveillance, Technology and Society Studies (Lavits);[289]
- European Data Protection Board (EDPB);[290]
- African Network of Data Protection Authorities (RAPDP);[291] and
- Central and Eastern Europe Data Protection Authorities (CEEC).[292]

3.1.6.1 The EU's General Data Protection Regulation

With its potential for extraordinarily high fines, the EU's GDPR impacts cross-border legal challenges on the internet in several ways. Most obviously, the GDPR claims a broad scope of application that goes well beyond the EU and imposes restrictions on when data may be transferred outside the EU. It also forces many non-EU entities to designate a representative in the EU and engages in 'standard setting' in that some multinationals have opted to adopt the GDPR as their standard of operation globally. Overall, however, it is the 'standard setting' quality of the GDPR that will generate the biggest impact; and the GDPR is being used as the 'blueprint' for widespread data privacy law reform around the world, from Argentina to New Zealand, and Kenya to Thailand.

> "The GDPR is used as the 'blueprint' for widespread data privacy law reform around the world, from Argentina to New Zealand, and from Kenya to Thailand."

The GDPR and its impact was one of the most commonly raised topics in both survey results and interviews, and was by far the most frequently mentioned legislative initiative. This is unsurprising, given the amount of global attention that the GDPR has received. In fact, it may be suggested that no other law-making initiative in modern history has attracted greater global attention.

There are at least six reasons the world has paid so much attention to the GDPR. First, as alluded to, the GDPR claims a broad scope of application that goes well beyond the EU. Article 3

---

284. International Federation of Library Associations and Institutions. *IFLA Statement on Privacy in the Library Environment*. Retrieved from https://www.ifla.org/publications/node/10056.

285. Center for Democracy and Technology. (2018, December 13). *CDT's Federal Baseline Privacy Legislation*. Retrieved from https://cdt.org/insight/cdts-federal-baseline-privacy-legislation-discussion-draft/.

286. International Conference on Data Protection and Privacy Commissioners. Retrieved from https://icdppc.org.

287. Asia Pacific Privacy Authorities. Retrieved from http://www.appaforum.org.

288. Red Iberoamericana de Proteccion de datos. Retrieved from http://www.redipd.es/index-ides-idphp.php.

289. Latin American Network of Surveillance, Technology and Society Studies. Retrieved from http://lavits.org/a-lavits/?lang=en.

290. European Data Protection Board. Retrieved from https://edpb.europa.eu/.

291. African Network of Data Protection Authorities. Retrieved from https://apdp.bj/.

292. Central and Eastern Europe Data Protection Authorities. Retrieved from http://www.ceecprivacy.org/main.php?s=2.

of the GDPR outlines the type of connecting factors that will trigger application of the GDPR.[293] To put it simply, the GDPR applies to any data controller or processor with an establishment in the EU, regardless of whether the processing takes place in the EU or not. It also applies to controllers or processors not established in the EU, in cases where they process the personal data of subjects who are in the EU – either by offering goods or services to such data subjects in the EU (a form of 'targeting test', discussed further in Chapter 4.1.5), or by monitoring their behavior within the EU. Finally, Article 3 contains a vague rule to the effect that the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

By the time the GDPR took effect, there was virtually no guidance as to the exact reach of its application. This resulted in an unhelpful degree of uncertainty among controllers and processors not established in the EU, and that would potentially be impacted by the GDPR's scope of application.

The loss of access to content

Several surveyed and interviewed experts noted that resources will be needed, and costs imposed, for ensuring compliance with the GDPR. In response, a number of small-to medium-sized businesses, as well as some larger actors, around the world have started using geo-location technologies (Chapter 4.2.1) to block users accessing their services from the EU.[294] Europeans seeking to access the website of the Chicago Tribune (www.chicagotribune.com), for example, are now met with the following message:

> "Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism."

The far-reaching 'extraterritorial' scope of application is by no means unique to the GDPR. It can also be found, in various forms, in data privacy laws around the world. At least on paper, however, the GDPR casts a wider net than most other data privacy laws, including the EU Data Protection Directive (DPD) that preceded it. Such broadening is likely to spread, as other legislative proposals are already embracing the language of GDPR's Article 3.[295] It would, therefore, not be surprising if the GDPR signals the start of increasingly broad claims of jurisdiction in data privacy laws around the world.

The second reason the world has paid so much attention to the GDPR is that it imposes significant limitations on cross-border data flows. This matter is explored in some detail below.

> "It would [...] not be surprising if the GDPR signals the start of increasingly broad claims of jurisdiction in data privacy laws around the world"

Third, while it is currently difficult to ascertain exact numbers, it is clear that the GDPR indirectly influences data privacy laws around the world, having already sparked reform discussions in some countries outside the EU. Given the experiences gained from the influence of the EU's DPD, one may safely assume that many countries around the world will be inclined to draw upon the GDPR when creating or reforming their own data privacy laws. (Thailand, Argentina, and Brazil are illustrations of this trend.) At the same time, one interviewed expert noted that it is very difficult for developing countries to comply with the GDPR due to the need for national regulatory authorities to be in place. Many developing countries simply do not have the necessary resources, expertise and independence to carry out the functions of such authorities. Developed countries ought to factor in such considerations when formulating the requirements that they impose on other states seeking interoperability.

As the GDPR continues to influence data privacy laws around the world, we can expect to see a degree of har-

---

293. See further: European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation* (adopted 16 November 2018), Taylor, M. (2018). *Transatlantic jurisdictional conflicts in data protection law: How the fundamental right to data protection conditions the European Union's exercise of extraterritorial jurisdiction.* (Dissertation). Utrecht University. Retrieved from https://dspace.library.uu.nl/handle/1874/367936 and Kuner, C., Bygrave, L.A. & Docksey, C. (Eds.). (2019). *Commentary on the EU General Data Protection Regulation.* Oxford: Oxford University Press.

294. Data Verified Joseph. *Websites not available in the European Union after GDPR.* Retrieved from https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr.

295. Thailand's Personal Data Protection Bill 2018.

monization. At the same time, the actual application of data privacy laws is always impacted by underlying values. The EU's application of the GDPR, for example, will be guided by the fact that the Charter of Fundamental Rights of the European Union specifically enshrines the protection of personal data.[296] Where other states adopt laws based on the GDPR, their application of those laws will be guided by those states' underlying values. This may result in differing applications of seemingly identical, or near identical, legal norms.

Fourth, as part of the mechanisms adopted to increase the effectiveness of the GDPR's enforcement, Article 27 of the GDPR requires a controller or processor not established in the Union, but falling within the GDPR's scope of application, to designate, in writing, a representative in the Union. This is part of the trend of 'rep localization' discussed in Chapter 4.1.3.

A fifth reason the GDPR has gained so much international attention is found in the heavy fines that may be imposed due to breaches. Article 83(5) calls for possible fines of up to €20 million, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher; this is also part of one of the major legal approaches discussed in Chapter 4.1.2.

Finally, the GDPR has gained international attention because some multinationals have opted to adopt it as their global standard of operation. In this 'standard setting' manner, the GDPR expands the data privacy rights enjoyed by users in states not bound by the GDPR.

As a regulation, the GDPR is directly applicable in EU Member States, unlike its predecessor, the DPD, which came into force in 1995. As a result, the EU is now meant to have one single data protection law, rather than a patchwork of data protection laws with a common origin in the DPD. But the GDPR does allow for a degree of national differences, so the choice of which EU Member State's law applies remains an important consideration in many situations.

The Council of Europe also modernized and adopted Convention 108 (Convention 108+) in 2018. The amended Convention 108 will have an important interaction with the GDPR, especially because the EU will be a party to it. As one interviewed expert noted, this will lead to the creation of a multinational forum in which non-EU states, that are parties to Convention 108+, can discuss the GDPR with the EU in a treaty environment. The interaction between such international instruments requires dialogue, coordination and cooperation.

3.1.6.2 The right to de-referencing

Discussions of a so-called 'right to be forgotten' (RTBF) – now predominantly referred to as the 'right to de-referencing' or 'de-indexing' – was largely sparked by the CJEU's interpretation of certain provisions of the EU's 1995 DPD in the 2014 *Google Spain* decision.[297] Essentially, the right to de-referencing allows individuals, in certain circumstances, to demand that search engines delist links to freely accessible web pages resulting from searches on their name. Yet, the exact delineations of the right to de-referencing vary across the states that have considered it.

The right has carried over into the GDPR. It has also gained some recognition beyond Europe, for example, in countries such as Argentina, India and South Korea. Canada's Privacy Commissioner has also taken the view that Canada's federal data privacy law (Personal Information Protection and Electronic Documents Act) provides for a right to de-indexing.[298]

Yet, the debate about the advantages and disadvantages of the right to de-referencing is far from over.[299] Courts in some states, such as Japan and China, have directly rejected claims involving the right to de-referencing. Concerns have been raised about the potential impact on freedom of expression and the concept of an open internet. In some states – particularly in Latin America – concerns about the right to de-referencing have been fueled by fears that it may allow perpetrators of recent human rights violations and corruption to hide their past abuses. This highlights the importance of recognizing the impact of cultural, social, political and historical backgrounds, and of viewing rights in their broader context.

---

296. *Charter of Fundamental Rights of the European Union*. (2000/C 364/01), Article 8.

297. Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. See further: van Alsenoy, B., Kuczerawy, A. & Ausloos, J. (2013),Search engines after 'Google Spain': Internet@Liberty or Privacy@Peril? ICRI Research Paper 15 TPRC 41. *The 41st Research Conference on Communication, Information and Internet Policy*. Retrieved from SSRN: https://ssrn.com/abstract=2321494 or http://dx.doi.org/10.2139/ssrn.2321494, and Lindsay, D. (2014). The "Right to be Forgotten" by search engines under data privacy law: A legal analysis of the Costeja ruling. *Journal of Media Law*, 6(2), 159; Lynskey, O. (2015). Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez. *The Modern Law Review*, 78(3), 522.

298. Masnick, M. (2018, October 16). Canadian Privacy Commissioner goes to court to determine if Canada can force Google to delete history. *Tech Dirt*. Retrieved from https://www.techdirt.com/articles/20181013/23132640833/canadian-privacy-commissioner-goes-to-court-to-determine-if-canada-can-force-google-to-delete-history.shtml.

299. See e.g.: Kohl, U & Rowland, D. (2017). Censorship and Cyberborders through EU Data Protection Law. In: Kohl, U. (Ed.). *The net and the nation state*. Cambridge: Cambridge University Press, 93-109.

> "In some states – particularly in Latin America – concerns about the right to de-referencing have been fueled by fears that it may allow perpetrators of recent human rights violations and corruption to hide past abuses."

The scope of the jurisdiction dimension of the right to de-referencing (i.e., the geographic extent of delisting) was not raised before the CJEU in the *Google Spain* matter. But this crucial cross-border issue has now come before the CJEU through an action brought against Google LLP by *Commission nationale de l'informatique et des libertés* (CNIL), France's data protection authority. In its action, the CNIL aimed to have right to be forgotten orders extended globally.

A similar matter came before the courts in Sweden. Though, unlike the CNIL, the Swedish data protection authority (*Datainspektionen*) argued in favor of a nuanced approach, under which the scope of the jurisdiction of the right to de-referencing would be guided by circumstances in individual cases.[300]

On January 10, 2019, Advocate General Szpunar issued his opinion on the CJEU matter. In his opinion, the Advocate General concluded that, in relation to the right to be forgotten, search engines "must take every measure available to it to ensure full and effective de-referencing within the EU."[301] Importantly, he went on to say that de-referencing of the search results should only apply inside the EU, though, he did not rule out the possibility that "in certain situations, a search engine operator may be required to take de-referencing actions at the worldwide level."[302] This is similar to the nuanced approach advocated for by the Swedish DPA.

On 24 September 2019, the CJEU ruled that:

> "where a search engine operator grants a request for de-referencing pursuant to [the relevant] provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to

300. Datainspektionen överklagar Google-dom. (2018, May 30). *DataInspektionen*. Retrieved from https://www.datainspektionen.se/nyheter/datainspektionen-overklagar-google-dom/.

301. Court of Justice of the European Union. (2019, January 10). *Advocate General Szpunar proposes that the Court should limit the scope of the de- referencing that search engine operators are required to carry out to the EU*. [Press Release]. Luxembourg. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002en.pdf.

302. Court of Justice of the European Union. (2019, January 10). *Advocate General Szpunar proposes that the Court should limit the scope of the de- referencing that search engine operators are required to carry out to the EU*. [Press Release]. Luxembourg. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002en.pdf.

the links which are the subject of that request."[303]

Importantly, the CJEU emphasized the importance of the fact that:

- "numerous third States do not recognise the right to de-referencing or have a different approach to that right."[304]
- "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[305]
- "the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world."[306]
- "While the EU legislature has [...] struck a balance between that right and that freedom so far as the Union is concerned [...], it must be found that, by contrast, it has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union."[307]
- "it is in no way apparent [...] that the EU legislature would [...] have chosen to confer a scope on the [relevant] rights [...] which would go beyond the territory of the Member States and that it would have intended to impose on an operator which, like Google, falls within the scope of that directive or that regulation a de-referencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States."[308]

Finally, it must be noted that the CJEU did not close the door to the nuanced approach envisaged by AG Szpunar and the Swedish data protection authority (as referred to above): "while, as noted [...] EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights [...], a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine."[309]

The implications of the outcome, as well as the reasoning that led to the outcome, are highly significant as it can be expected that the EU's approach will be influential or even standard setting.

3.1.6.3 Data privacy restriction of cross-border data transfers

Many aspects of modern society, such as international financial transactions, travel, communication, and indeed research,[310] depend upon cross-border data transfers. This dependence will only increase with ongoing developments such as the Internet of Things (see further Chapter 3.3.4). At the same time, data transfers across borders commonly involve a degree of loss of control over that data, and an erosion of direct influence of the body tasked with upholding data protection in the country from which the data originates. This conundrum has been a central issue in international data privacy initiatives since 1980, when the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were released.[311]

The longstanding debate on the circumstances under which personal data may be transferred across borders has continued in recent years[312] –

---

303. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 74. See further: van Calster, G. (2019). Court of Justice in Google sees no objection in principle to EU 'Right to be forgotten' leading to worldwide delisting orders. Holds that as EU law stands, however, it is limited to EU-wide application, leaves the door open to national authorities holding otherwise. *GAVC Law*. Retrieved from https://gavclaw.com/2019/09/25/court-of-justice-sees-no-objection-in-principle-to-eu-right-to-be-forgotten-leading-to-worldwide-delisting-orders-holds-that-as-eu-law-stands-however-it-is-limited-to-eu-wide-application-leave/; and Svantesson, D. (2019, September 24). The Court of Justice of the European Union steers away from global removal orders. *LinkedIn*. Retrieved from https://www.linkedin.com/pulse/court-justice-european-union-steers-away-from-global-svantesson/.

304. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 59.

305. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 60

306. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 60

307. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 61

308. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 62

309. Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), para 72. This nuanced approach was initially canvassed in detail in: Svantesson, D. J. B. (2015). The *Google Spain* case: Part of a harmful trend of jurisdictional overreach. *EUI Working Paper RSCAS* 2015/45. Retrieved from https://cadmus.eui.eu/bitstream/handle/1814/36317/RSCAS_2015_45.pdf?sequence=1.

310. Bentzen, H. B. et al., (2019). Are requirements to deposit data in research repositories compatible with the European Union's General Data Protection Regulation?, *Annals of Internal Medicine*, 170(5), 332-334

311. OECD. *OECD Guidelines on the protection of privacy and transborder flows of personal data*. Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

312. See e.g.: Toy, A. & Gunasekara, G. (2019). Is there a better option than the data transfer model to protect data privacy? *University of New South Wales Law Journal*, 42(2), 719-746.

most notably, in the context of transatlantic data transfers. The CJEU handed down a ruling in 2015 that invalidated the Safe Harbour arrangement which, until then, had governed data transfers between the EU and the US.[313] A period of great uncertainty followed, and in mid-2016, the Safe Harbour scheme was replaced by a new arrangement named Privacy Shield.

In 2018, the High Court of Ireland referred to the CJEU questions relating to another basis for cross-border data transfers: so-called Standard Contract Clauses (SCC).[314] Essentially, the matter relates to whether EU law allows SCCs, in their present form, as a basis for the transfer of personal data from the EU to the US.

> "Compliance with Convention 108+ ensures compliance with most, but not all, of the GDPR's requirements. Thus, it remains to be seen whether a country's compliance with Convention 108+ convinces the EU to view that country's data privacy laws as meeting the GDPR's adequacy test."

The interaction between the GDPR and the Council of Europe's Convention 108+ raises interesting questions in the context of cross-border data transfers, and more generally, about the interoperability between different regimes. Compliance with Convention 108+ ensures compliance with most, but not all, of the GDPR's requirements. Thus, it remains to be seen whether a country's compliance with Convention 108+ would convince the EU to view that country's data privacy laws as meeting the GDPR's adequacy test.

In the Asia-Pacific context, the Asia-Pacific Economic Cooperation (APEC) endorsed its Cross-Border Privacy Enforcement Arrangement (CPEA) in 2010.[315] Participation in the CPEA – a multilateral framework for regional cooperation in enforcing privacy laws – is open to any privacy enforcement authority in an APEC member economy. Current member authorities come from: Australia, New Zealand, the US, Japan, Hong Kong, Canada, Korea, Mexico, Singapore, Philippines and Chinese Taipei.

The APEC Cross-Border Privacy Rules (CBPR) system is also gaining momentum. The CBPR is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies.[316] To a degree, it bears similarities to the GDPR's Binding Corporate Rules (BCR) system for cross-border data transfers.

One interviewed expert noted that there are some suggestions that the CBPR system may be turned into an independent international system, and that the CBPR is recognized in other initiatives as a good model – for example, in the context of the United States-Mexico-Canada Agreement on digital trade and in the context of Japan's new Data Protection Law.

China released a Draft Regulation on Cross-Border Transfer of Personal Information in June 2019, with restrictions on the transfer of personal information overseas, if such information risks undermining national security and public interests.[317]

Coordination is urgently needed as several states move forward with their own assessments of other states' data privacy laws. On July 17, 2017, for example, the Colombian DPA launched a consultation on draft regulations to reform cross-border data transfer rules, and identified countries that have 'adequate' data protection rules as a necessary condition to allow such data transfers.[318] The regulations introduce requirements that are in line with Law 1581,[319] passed in 2012, which introduced the requirement for personal data to be adequately protected in cross-border data transfers.[320]

A further recent initiative was a proposal by the Japanese government during the G20 in Osaka in June 2019 for the adoption of a Data Free Flow with Trust concept, calling for international rules to permit the free movement of data across borders.[321]

---

313. Case C-362/14 Maximillian Schrems v Data Protection Commissioner.

314. Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems.

315. Asia-Pacific Economic Cooperation. *APEC Cross Border Privacy Enforcement Arrangement.* Retrieved from https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

316. Cross Border Privacy Rules System. Retrieved from http://cbprs.org.

317. Caiyu, L. (2019, June 13). China sets cross-border data flow rules. *Global Times.* Retrieved from http://www.globaltimes.cn/content/1154091.shtml.

318. Nelson-Daley, R. (2017, July 27). Colombia: Amended draft transfers regulation seeks to 'address main concern' regarding adequate jurisdictions. *DataGuidance.* Retrieved from http://www.dataguidance.com/colombia-amended-draft-data-transfers-regulation-addresses-main-concerns-regarding-list-adequate-jurisdictions/.

319. Sanlate, G., Gordon, P., Méndez, S.M &, Varela, J. C. (2013, July 29). Colombia adopts regulations to implement its data protection laws. *Littler.* Retrieved from https://www.littler.com/publication-press/publication/colombia-adopts-regulations-implement-its-data-protection-laws.

320. Internet & Jurisdiction Policy Network. (2017, July). Colombia establishes list of countries with adequate data protection for cross-border transfers. *I&J Retrospect Database.* Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6188_2017-07.

321. Sugiyama, S. (2019). Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20. *Japan Times.* Retrieved from https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/#.XY73EGXA5II.

3.2

Security

The internet gives rise to numerous security issues, ranging from personal security to national security. As the internet continues to play an increasingly central role in society, internet security will only become more important. In a world where more and more things are 'connected', the interdependence between online security from offline security is increasing.

The significance of cybersecurity is clearly reflected in the World Economic Forum's Global Risks Report 2018.[322] Among the Top 10 risks in terms of likelihood, 'cyberattacks' ranked 3rd and 'data fraud or theft' ranked 4th. This is particularly serious given that, in terms of impact, 'cyberattacks' were also ranked 6th among the top 10 risks. Such interconnectedness is palpable, as actions in one state impact other states, giving rise to many cross-border legal challenges in the context of security. These include:

- Countries may struggle to collaborate on, and coordinate, security efforts;
- Criminals may benefit significantly from jurisdictional obstacles to the detection, investigation and prosecution of their misdeeds;
- Ensuring access to digital evidence often depends on the cooperation of private actors, which has sparked a re-examination of the role they hold;
- States seeking to place their citizens under surveillance may need the voluntary or coerced cooperation of foreign privately-operated platforms, and breaking encryption may depend on the cooperation of foreign hardware manufacturers;
- Data breaches by a company in one state may impact a worldwide group of users; and
- States may adopt e-government solutions that involve storing critical data on servers in foreign countries.

It is also increasingly difficult to distinguish between the regulation of security and other fields of regulation. Security requirements, for example, are a standard aspect of many data privacy regimes. In that regard, data privacy and security are two sides of the same proverbial coin, even though the two are often portrayed in opposition to one another.

In the online security field, it is sometimes difficult to distinguish between civil wrongs, criminal offenses, acts of terrorism and even military aggression – and from this, a range of complications arise.[323] This contributes to making regulation – and especially international consensus on regulatory responses – difficult to achieve.

Some distinctions are developing, though. In the context of access to digital evidence, for example, one interviewed expert noted that governments are increasingly emphasizing the need for different processes for national security matters, as compared to traditional criminal matters.

It is clear that the area of internet security is complex and multifaceted.

There are some examples of industry members working together to improve cybersecurity including:

- The launch of the **Council to Secure the Digital Economy** (CSDE) in **2018** by international internet service providers.[324] The members of CSDE collaborate with the aim of securing digital infrastructure. CSDE released its International Anti-Botnet Guide in 2018.
- The **Cyber Threat Alliance** has industry members who share threat intelligence to improve cybersecurity and resilience.[325]
- **Cybersecurity Tech Accord** has over 100 industry members seeking to share cybersecurity capacities.[326]
- The global **Forum of Incident Response and Security Teams** (FIRST) with 400 members from Africa, the Americas, Asia, Europe and Oceania.[327]
- The **Anti-Phishing Working Group** engages law enforcement, industry, NGOs and governments to undertake data exchange, research and public awareness in order to respond to cybercrime.[328]
- The **Messaging, Malware and Mobile Anti-Abuse Working Group** (M3AAWG) has industry members working together to combat cybercrime.[329]

---

322. World Economic Forum. (2018). *The Global Risks Report 2018.* (13th ed.). Retrieved from http://reports.weforum.org/global-risks-2018/.
323. For an interesting discussion see: Haataja, S. (2019). *Cyber attacks and international law on the use of force: The turn to information ethics.* New York: Taylor & Francis Ltd.
324. Council to Secure the Digital Economy. Retrieved from https://securingdigitaleconomy.org.
325. Cyber Threat Alliance. Retrieved from https://www.cyberthreatalliance.org.
326. Cybersecurity Tech Accord. Retrieved from https://cybertechaccord.org/accord/.
327. Forum of Incident Response and Security Teams. Retrieved from https://www.first.org.
328. Anti-Phishing Working Group. Retrieved from https://apwg.org.
329. Messaging, Malware and Mobile Anti-Abuse Working Group. Retrieved from https://www.m3aawg.org.

Yet, there appears to be a need for further and deeper collaboration. For example, one surveyed expert suggested that, given the borderless nature of cybercrime (in particular, malware), increased global reporting and the creation of a malware lab and library could be beneficial. As explained by this expert, understanding the evolution and trends, based on the big data that could be generated, would have advantages over the current countless silos of relevant information housed within governments, universities and industry.

3.2.1

Cybercrime

Every step from identification, to investigation, prosecution and extradition,[330] of cybercrime and cybercriminals raises jurisdictional issues. In fact, addressing cybercrime is impossible without cross-border cooperation and coordination, and still then, there are many obstacles. Effective law enforcement, especially if it demands cross-border cooperation, requires significant resources that are seldom at the disposal of developing countries. Furthermore, a state's criminal law goes to the core of that state's values and traditions, so an act outlawed in one state may be lawful in another.

There are still many acts that are recognized as crimes in virtually all legal systems, and the domestic laws of many states now deal specifically with cybercrimes[331] – and have done so for some time. As a result, offenders are significantly less likely to be able to rely on gaps in the law.

Cases like the infamous 2000 'ILOVEYOU' computer worm – whose creator had to be let go because the Philippines did not have laws against writing malware at that time – are far less likely to arise today. Looking forward, further capacity building and gap elimination must continue to be included among the goals of cross-border cooperation and coordination in the field of cybercrime.

Through its Global Complex for Innovation (IGCI) in Singapore, Interpol seeks to be a global coordination body for the detection and prevention of digital crimes.[332] Interpol also has a dedicated Information and Communications Technology Law team that specializes in legal projects related to ICT law; and it is currently engaged in several projects.[333]

In the context of the Europe Union, Eurojust[334] and Europol's European Cybercrime Centre[335] set up in 2013, together with its Joint Cybercrime Action Taskforce (J-CAT) launched in 2014,[336] gained particular praise from some of the interviewed experts.

The Council of Europe's Convention on Cybercrime (the 'Budapest Convention') is the most significant international instrument addressing cybercrime.[337] This important instrument serves as a guideline for any country developing comprehensive national legislation against cybercrime, and as a framework for international cooperation between state parties to this treaty.[338] In particular, it addresses infringements of copyright, computer-related fraud, child pornography and violations of network security. It contains additional provisions on a range of powers and procedures, including the search of computer networks and interception. Importantly, as one interviewed expert emphasized, the 'Budapest Convention' incorporates human rights safeguards and makes specific reference to international human rights instruments. As of September 30, 2018, the 'Budapest Convention' is in effect in 64 countries around the world.[339]

Other relevant initiatives include, the:

- Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in **Africa** (**2011**);
- **Commonwealth** Model Law on

---

330. Mann, M., Warren, I. & Kennedy, S. (2018). The legal geographies of transnational cyber-prosecutions: extradition, human rights and forum shifting. *Global Crime*, 19(2), 107-124. Retrieved from https://www.tandfonline.com/doi/full/10.1080/17440572.2018.1448272.

331. See: United Nations Conference on Trade and Development. *Cybercrime legislation worldwide*. Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx. See further, for example: Walden, I. (2016). *Computer crimes and digital investigations*. (2nd ed.). New York: Oxford University Press.

332. Interpol. *Cybercrime*. Retrieved from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

333. Interpol. *ICT Law Projects*. Retrieved from https://www.interpol.int/About-INTERPOL/Legal-materials/ICT-Law-Projects/Overview.

334. The European Union's Judicial Cooperation Unit. Retrieved from http://www.eurojust.europa.eu/Pages/home.aspx.

335. Europol. *European Cybercrime Centre - EC3*. Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

336. Europol. *Joint Cybercrime Action Taskforce (J-CAT)*. Retrieved from https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.

337. See further: Council of Europe. *Action against cybercrime*. Retrieved from https://www.coe.int/en/web/cybercrime/home.

338. Council of Europe. *Budapest Convention and related standards*. Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

339. Council of Europe. *Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=9zMAKGj4.

Computer and Computer Related Crime (**2002**);[340]
- **United Nations** Convention against Transnational Organized Crime (**2000**) and its three protocols;
- **Stanford** Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (**1999**);
- **Inter-American** Convention on Mutual Assistance in Criminal Matters (**1992**); and
- **European** Convention on Mutual Assistance in Criminal Matters (**1959**).

Established organizations are increasingly engaging with these issues, as well. In 2018, for example, the World Economic Forum established a Centre for Cybersecurity.[341] There are also agencies dedicated to cybersecurity, such as the EU Agency for Network and Information Security (ENISA).[342]

3.2.1.1 Enforcement difficulties due to jurisdiction as a hurdle

It has been noted that cybercrime is largely underreported, and that "among the offences reported and recorded by law enforcement authorities, only an infinitesimal part is eventually investigated. Of these, only a very small fraction is prosecuted, and of these again, only a few are adjudicated."[343]

Faced with this situation, it is only natural that some commentators speak of a *de facto* impunity of the perpetrators of cybercrimes.[344]

Some of the reasons for the low prosecution rate of cybercriminals are highlighted above, though, obvious jurisdictional challenges also play a role. As noted by Advocate General Wathelet in Case C-618/15 "[t]he issue of crime committed on the internet ('cybercrime') is not a straightforward one inasmuch as, since the internet is a network which is by definition universal, the location of such crime, be it the causal event or the loss sustained, is particularly difficult to determine."[345] The difficulty of ascertaining the location of crime committed on the internet may be a major complication when applying traditional rules of jurisdiction. Furthermore, in cases where the offender is in another country, prosecution may be limited by the degree to which offenders may be extradited from the country in question. This complication may, of course, arise in relation to any form of criminal activity, but cybercrime is particularly prevalent as a cross-border activity.

The cybercrime landscape is forever changing and new trends are frequently emerging. For example, Europol's 2018 Internet Organised Crime Threat Assessment notes that, "a significant volume of public reporting increasingly attributes global cyber-attacks to the actions of nation states".[346] This further undermines the likelihood of successful prosecution.

> "The difficulty of ascertaining the location of crime committed on the internet may be a major complication when applying traditional rules of jurisdiction."

3.2.1.2 Darknet – a criminal haven beyond national jurisdiction?

While references to the so-called 'Darknet' are commonplace, an in-depth understanding of it is less common. The term 'Darknet' has a long history but has recently gained prominence due to illegal trade – for example, via the Silk Road[347] – carried out on parts of the internet that are purposefully closed from public view, or through hidden networks whose architecture is superimposed on the internet.

Transactions carried out on the Darknet may make attribution difficult and may complicate the application of location-based jurisdictional connecting factors.

The Darknet is playing an increasing

---

340. See further: Brown, C.S.D. (2015). Investigating and prosecuting cyber crime: Forensics dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9:55–119.

341. World Economic Forum. (2018). *Centre for Cybersecurity*. https://www.weforum.org/centre-for-cybersecurity.

342. European Union Agency for Network and Information Security. *About ENISA*. Retrieved from https://www.enisa.europa.eu/about-enisa.

343. Kleijssen, J. & Perri, P. (2016). Cybercrime, evidence and territoriality: Issues and options. *Netherlands Yearbook of International Law*, 47, pp. 153-154.

344. See e.g.: Kleijssen, J. & and Perri, P. (2016). Cybercrime, evidence and territoriality: Issues and options. *Netherlands Yearbook of International Law*, 47, p. 154.

345. Case C-618/15 Concurrence Sàrl v Samsung Electronics France SAS and Amazon Services Europe Sàrl, para 2.

346. Europol. (2018). *Internet Organised Crime Threat Assessment 2018*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf, p. 7.

347. Wikipedia. *Silk Road (marketplace)*. Retrieved from https://en.wikipedia.org/wiki/Silk_Road_(marketplace). See further: Mann, M. & Warren, I. (2018). The digital and legal divide: Silk Road, transnational online policing and Southern criminology. In Carrington, K., Hogg, R., Scott, J. & Sozzo, M. (Eds.), *The Palgrave handbook of criminology and the global south* (pp.245-260). Cham, Switzerland: Palgrave Macmillan. Retrieved from http://dro.deakin.edu.au/view/DU:30105929.

role in the distribution of the vilest materials. As Europol's 2018 Internet Organised Crime Threat Assessment notes: "Although most CSEM [Child Sexual Exploitation Material] is still shared through P2P platforms, more extreme material is increasingly found on the Darknet."[348] More broadly, the same Threat Assessment Report notes, that:

> "The Darknet will continue to facilitate online criminal markets, where criminals sell illicit products in order to engage in other criminal activity or avoid surface net traceability. In 2017, law enforcement agencies shut down three of the largest Darknet markets: AlphaBay, Hansa and RAMP. These takedowns prompted the migration of users towards existing or newly established markets, or to other platforms entirely, such as encrypted communications apps."[349]

While statistics on migration are currently lacking, it is possible that, as major online platforms enforce stronger rules on the content their users post, illegal or objectionable content will migrate to smaller platforms, over which it is often harder to claim jurisdiction.

> "The Darknet is playing an increasing role in the distribution of the vilest materials."

3.2.2

Access to digital evidence

It is a state's obligation to carry out effective law enforcement in accordance with fundamental rights. To be effective, law enforcement needs adequate access to evidence. Such access is essential both for the conviction of criminals, and for the protection of those wrongly accused.

As several interviewed experts noted, the importance of digital evidence has increased tremendously over the last decade. Today, information that may amount to relevant evidence – both in relation to specific cybercrimes and traditional crimes – is often stored in cloud structures outside the state of the law enforcement agency that needs access to the data in question. This is not just the case in relation to the cloud structures of the major internet companies, but for millions of different app providers, as well. Further, particular issues arise in certain industries.[350] This diversity puts pressure on the scalability of any proposed solutions.

Ascertaining the location of the data may be difficult, or in some cases, impossible. Problems that arise include situations where:

1. the location of the data cannot be ascertained within a reasonable timeframe and with reasonable measures; and
2. the data required is split over servers in more than one location.

Even where the location of data may be ascertained, the mobility of data makes it possible to manipulate its location in order to hinder law enforcement measures.

3.2.2.1 Need for reform of the Mutual Legal Assistance (MLA) system

The Mutual Legal Assistance (MLA) system is the principal mechanism for law enforcement cross-border access to evidence.[351] It is based on a system of agreements between two or more states for the purpose of gathering and exchanging information to enforce public or criminal laws.

The MLA system is plagued by gaps as not all states have MLA agreements. Furthermore, it is widely acknowledged – and many interviewed experts emphasized – that the MLA structure cannot support the number of requests made under it. Some interviewed experts observed that there is not enough guidance to file requests, leading to requests being rejected for avoidable mistakes. Improvements of the MLA system – and indeed any other developments in this field – should, therefore, incorporate clear and simple guidance to ensure correct filings.

Given the above concerns, even an im-

---

348. Europol. (2018). *Internet Organised Crime Threat Assessment 2018*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf, p. 7.

349. Europol. (2018). *Internet Organised Crime Threat Assessment 2018*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf, p. 8.

350. For example, in 2017 the American Library Association published its Suggested Guidelines: How to respond to law enforcement requests for library records and user information. Retrieved from http://www.ala.org/advocacy/privacy/lawenforcement/guidelines.

351. See further: Kent, G. (2014, February 14). *Sharing investigation specific data with law enforcement - An international approach*. Stanford Public Law Working Paper. Retrieved from: http://dx.doi.org/10.2139/ssrn.2472413; and Osula, M. (2017). *Remote search and seizure of extraterritorial data*. Tartu: University of Tartu Press.

proved MLA system would not solve the challenges faced in satisfying law enforcement's need for cross-border access to evidence. For example, a 2014 Council of Europe assessment of the functioning of MLA provisions concluded, that:

"The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence."[352]

Despite its weaknesses, there are few calls for the MLA structure to be abandoned. The most common calls are instead for it to be supplemented with a system for direct requests to data holders, and for the MLA system to be made more efficient. Work on the latter is being carried out by, for example, the Council of Europe,[353] and Interpol.[354]

3.2.2.2 Law enforcement access to data outside the MLA structure

Private parties that hold data – typically major internet companies – are often exposed to the requirements of multiple legal systems, due to their presence in multiple markets. Special complications may arise if the corporation holding data, that is sought as evidence, is a company wholly owned by a state other than the state seeking access to the data. A matter in US courts provides a recent example of this.[355]

As in many other areas, relevant law, and how the law is applied, differs across legal systems. A common feature, however, is that a state's requirements for when its law enforcement agencies may access cross-border data often differ from the requirements imposed on foreign law enforcement agencies seeking access to data stored by private parties in that same state's jurisdiction.

Private parties that hold data may be put in a position where compliance with one state's laws unavoidably results in a direct violation of another state's laws because they are exposed to multiple legal systems with varying rules, for example, with regard to notification requirements.[356] Such situations are clearly harmful for all stakeholders, and there is broad agreement that such situations should be minimized or, if possible, eliminated.

The relevant (public) international law rules and concepts are an important part of the discussion, though they are not well understood, and often phrased in unjustifiably absolutist terms more suited for the political arena, than as guidance on legal matters. This legal uncertainty is not sustainable. In particular, the lack of clear cooperation frameworks hinders effective law enforcement and undermines due process. It also encourages mandatory data localization approaches that are technically difficult to implement, and can have detrimental impacts on the cloud economy and human rights.

---

352. Council of Europe, Cybercrime Convention Committee. (2016, September 16). *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*. T-CY (2016) 5, p. 9. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

353. Council of Europe. *MLA Council of Europe Standards*. Retrieved from https://www.coe.int/en/web/transnational-criminal-justice-pcoc/MLA-council-of-europe-standards.

354. Interpol. (2018, November 12). *Interpol's e-MLA initiative focus of EU expert meeting*. Retrieved from https://www.interpol.int/News-and-media/News/2018/N2018-134.

355. In re: Grand Jury Subpoena, No. 18-3071 (D.C. Cir. 2019). Retrieved from https://www.cadc.uscourts.gov/internet/judgments.nsf/DA9F6932C876287F852583680053B08B/$file/18-3071-1764819.pdf.

356. Osula, A-M. & Zoetekouw, M. (2017). The notification requirement in transborder remote search and seizure: Domestic and international law perspectives. *Masaryk University Journal of Law and Technology*, 11(1), 103-128.

This is a pivotal time, as several important projects are underway to address the noted complications:

There are important developments underway in relation to the **Budapest Convention**. Most relevantly, work is underway on a 2nd Additional Protocol.[357] A Guidance Note regarding production orders for subscriber information was published in **2017**,[358] and working documents relating to criminal justice access to data in the cloud have been issued.[359] Work is also underway aimed at addressing the relationship between the Budapest Convention on the one hand, and the EU's forthcoming law in the field on the other hand.[360]

In **February 2019**, the **United Nations Office on Drugs and Crime** (UNODC), the **United Nations Counter-Terrorism Committee Executive Directorate** (CTED) and the **International Association of Prosecutors** (IAP) jointly released a Practical Guide to Requesting Electronic Evidence Across Borders, targeted to investigators and prosecutors.[361]

In **December 2018, Australia**'s controversial Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 received Royal Assent and became law. The law has gained worldwide attention due to its far-reaching negative impact on encryption. Its extensive jurisdictional reach has gained less attention: anyone, anywhere in the world, who operates a website with at least one end-user in Australia is subject to Australian jurisdiction. Further, a party caught by the Act might be compelled to hand over data on its overseas users and to grant access to devices in other countries.

In **April 2018**, the **European Commission** published the Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings,[362] and the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.[363] These proposed instruments complement each other and must be read together. In essence, the combined effect of the proposed Directive and Regulation is to implement a scheme under which service providers – including foreign service providers – would be obligated to designate a legal representative in the Union. This is combined with the creation of a European Production Order and a European Preservation Order. Several interviewed experts cited differences that exist among EU Member States as a potential challenge. In the context of the instruments discussed here, one interviewed expert questioned whether EU countries with weaker standards, such as Poland and Hungary, will be able to have their demands enforced in other EU countries with higher standards. On **December 7, 2018**, the **EU Council** agreed on its position on the proposed Regulation,[364] and on **March 8, 2019** the **EU Council** agreed on its position on the proposed Directive.[365] As noted by one surveyed expert, these EU initiatives are not only relevant from the point of view of the possibilities they create for law enforcement, but they redefines the role of private actors (i.e. the service providers) in law enforcement in making them de facto guardians of fundamental rights; a role not officially defined in the proposal. This is a fundamental shift in their position vis-a-vis law enforcement and their clients.

---

357. For the latest developments at the time of writing see: Council of Europe, Cybercrime Convention Committee. (2019, July 8). *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime – State of Play*. Retrieved from https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff.

358. Council of Europe, Cybercrime Convention Committee. *T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)*. Retrieved from https://rm.coe.int/16806f943e.

359. Council of Europe, Cybercrime Convention Committee. (2016, September 16). *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*. T-CY (2016)5, p. 9. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

360. Council of Europe. (2019, April 29). *Use of a 'disconnection clause' in the second additional protocol to the Budapest Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/dlapil/-/use-of-a-disconnection-clause-in-the-second-additional-protocol-to-the-budapest-convention-on-cybercri-1.

361. United Nations Office on Drugs and Crime. (1 February 2019). *UNODC and partners release Practical Guide for Requesting Electronic Evidence Across Borders*. Retrieved from https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html.

362. European Commission. (2018, April 17). *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*. COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.

363. European Commission. (2018, April 17). *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*. COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

364. Council of the European Union. (2018, December 7). *Regulation on cross border access to e-evidence: Council agrees its position*. [Press Release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

365. Council of the European Union. (2019, March 8). *E-evidence package: Council agrees its position on rules to appoint legal representatives for the gathering of evidence*. [Press Release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/.

At least partially driven by the controversy surrounding the dispute in Microsoft Corp. v. United States,[366] the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943) was enacted in the **US** in **2018**.[367] A primary function of the CLOUD Act is to amend the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel US-based technology companies, via warrant or subpoena, to provide requested data stored on servers, regardless of whether the servers are in the US or on foreign soil. The CLOUD Act also provides for a structure under which governments outside the US may seek access to electronic data held by communications-service providers in the US, for the purpose of combating serious crime. One interviewed expert noted that the CLOUD Act will be effective on a very limited basis but may incentivize other states to raise or maintain standards in order to meet its requirements. Another observed that the CLOUD Act expressly refers to the standards set by the Budapest Convention, and therefore constitutes an incentive for states to accede to the Budapest Convention. Yet another stressed that the CLOUD Act is calculated to give the US government maximum flexibility in deciding which countries will be given the opportunity to make direct demands on US providers.

On **January 9, 2018**, the Court of Appeal of **British Columbia** ruled that non-Canadian companies were required to comply with production orders of provincial courts and hand over data to law enforcement, as long as the company has 'virtual presence' in the province, and even if they are not incorporated in the country.[368] It was contended that the lack of difference between physical and virtual presence could have major implications beyond production orders.[369]

Since **2012**, the legal issues surrounding law enforcement access to digital evidence has been a focus area of the **Internet & Jurisdiction Policy Network**. As one of its three Thematic Programs, the Data & Jurisdiction workstream has sought to tackle the issue of how transnational data flows and the protection of privacy be reconciled with lawful access requirements to address crime.[370] Due to the active involvement of participants from a broad range of stakeholders, significant progress has been made toward the development of an operational framework.[371]

In discussions of initiatives such as those listed above, it is important to distinguish between jurisdiction over the offense under investigation, on the one hand, and jurisdiction over the evidence needed for the investigation, on the other. The Budapest Convention clearly articulates such a distinction.[372] Article 22, the provision that addresses jurisdiction in general terms, relates only to jurisdiction over the offenses prescribed in the Cybercrime Convention (i.e., Articles 2- 11), and does not govern jurisdiction over the evidence.

The first matter of jurisdiction that arises in a criminal investigations is whether the investigator (be it the police, a prosecutor or an investigative judge) has jurisdiction over the offense to be investigated. On a theoretical level, the answer to that question will depend on both domestic law on jurisdiction and international law. In practice, though, investigators will (often legitimately) assume that the domestic jurisdictional law they work with is in line with international law. Thus, on a practical level, domestic jurisdictional law is typically determinative.

If it is concluded that the investigator has jurisdiction over the offense to be investigated, another type of jurisdictional issue arises: Does the investigator have jurisdiction to take the investigative measures that it wishes to pursue? Traditionally, this has been viewed as a matter of 'enforcement jurisdiction' and has, therefore, been grouped together with, and subjected to, the same restrictions as completely different types of actions, such as law enforcement agents from one country kidnapping suspects in other countries, as in the famous *Eichmann* case. More recently, investigative measures have been treated as something markedly different, and treating 'investigative jurisdiction' as a category distinct from enforcement jurisdiction is gaining recognition.

In addition to these jurisdictional issues, situations in which law enforcement agencies seek access to data held by private parties, such as internet intermediaries, give rise to a range of other complex considerations.

---

366. Wikipedia. *Microsoft Corp. v United States.* Retrieved from https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States.

367. See further: Daskal, J. (2019, January 31). *Unpacking the CLOUD Act*. Retrieved from https://eucrim.eu/articles/unpacking-cloud-act/.

368. British Columbia (Attorney General) v. Brecknell 2018 BCCA 5. Retrieved from https://www.canlii.org/en/bc/bcca/doc/2018/2018bcca5/2018bcca5.html?resultIndex=1.

369. Internet & Jurisdiction Policy Network. (2018, January). Canadian provincial Court of Appeal rules courts can demand data from non-Canadian companies if they have 'presence' in the country. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6681_2018-01.

370. Internet & Jurisdiction Policy Network. *Data and Jurisdiction*. Retrieved from https://www.internetjurisdiction.net/work/data-jurisdiction.

371. In addition there are other, partially overlapping, initiatives such as: Evidence2e-CODEX. Retrieved from https://evidence2e-codex.eu/ and Cross-Border Data Forum. Retrieved from https://www.crossborderdataforum.org/.

372. Council of Europe Convention on Cybercrime (ETS No. 185), opened for signature on 23 November 2001 (entered into force 1 July 2004).

DATA
& JURISDICTION PROGRAM

Stakeholders in the Internet & Jurisdiction Policy Network work together in three policy Programs: the Data & Jurisdiction Program, Content & Jurisdiction Program, and Domains & Jurisdiction Program. The Programs allow members to informally coordinate policies and jointly develop proposals for operational Norms, Criteria and Mechanisms. The Data & Jurisdiction Program currently focusses on access to cross-border electronic evidence towards the common objective of defining substantive and procedural standards that allow relevant authorities from specific countries in investigations regarding certain types of crimes, with clear nexus to directly submit structured and due process-respecting requests to private companies in another country, to obtain the voluntary disclosure of user data.[373] The Data & Jurisdiction Program's current work is based on the Ottawa Roadmap of the Internet & Jurisdiction Policy Network that produced concrete proposals for operational Norms, Criteria, and Mechanisms in 2019. It addresses the following issues:[374]

- Standards: Statutory requirements to ensure high and robust human rights protections, while meeting lawful requests from law enforcement, and providing legal clarity to those receiving requests;
- Qualifying regimes and requests: Streamlined access to data requires both a qualifying regime and qualifying individual requests;
- Countries: Evaluation and review procedures to determine eligible countries, while seeking to improve practice for requests to all countries;
- Authorities: Competent authorities, defined by nation or for units within a nation, for issuing cross-border requests;
- Scope: Types of criminal investigations to be considered within scope;
- Users: Provisions regarding users who are not nationals or residents of the requesting country;
- Requests: Content and structure of properly documented requests, with proper legal authorization, including judicial approval where possible;
- Due process: Guarantees regarding, *inter alia*, user notification, capacity to object, recourse and redress. Consideration of notice to relevant non-requesting nations;
- Companies: Voluntary nature of disclosure (although similar factors apply to compulsory regimes) and procedures in case of doubt;
- Data: Tailored rules for categories of data, such as content and non-content data, or for especially sensitive information;
- Data location: How to deal with data stored digitally, providing weight to factors beyond its physical location;
- Scalability: Framework extension over time, beyond initial participating countries, to respond to increasing magnitude and diversity of requests;
- Data preservation: Provisions to preserve data for an individual investigation, before a full request for data can be made; and
- Capacity: Providing training and staffing to meet the regime's requirements.

---

373. For the concrete proposals, see: Internet & Jurisdiction Policy Network. *Data & Jurisdiction Program Operational Approaches*. Retrieved from http://internetjurisdiction.net/Data-Jurisdiction-Program-Operational-Approaches.
For the latest work plan, see 3rd Global Conference of the Internet & Jurisdiction Policy Network. (2019, June 3-5). *Berlin Roadmap*. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/Berlin-Roadmap-and-Secretariat-Summary-3rd-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf

374. 2nd Global Conference of the Internet & Jurisdiction Policy Network. (2018, February 26-28). *Ottawa Roadmap*. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/ Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf, p. 6-7.

This illustrates the complexity of law enforcement accessing evidence stored in the cloud and outside of the state seeking access to the evidence. As has been expressed in literature and policy documents for some time, and as has been strongly emphasized in the stakeholder interviews carried out for this Report, there is a clear need for legal clarity as to the roles, responsibilities, authorities and limitations for all stakeholders in providing law enforcement with access to digital evidence.

Substantial discussions on this topic have focused on situations involving law enforcement bodies seeking access to digital evidence. But other governmental bodies – such as consumer protection bodies, human rights bodies and data protection bodies – may seek such access in similar circumstances. The question then arises whether considerations made in the context of law enforcement should apply equally to such governmental bodies. This is a topic that will only grow in importance, and one that requires urgent attention.

3.2.2.3 Moving from data location as a connection factor, and a recognition of the role of interest balancing

Until recently, discussions of jurisdiction in the context of law enforcement access to data held overseas strongly focused on the implications of territorial sovereignty. It was commonly assumed that if a law enforcement agency in state A gains access to evidence held on a server in state B, this somehow violates state B's sovereignty, regardless of whether state B:

1. is aware of the data;
2. can access the data; or
3. has any discernible interest in the data.

This overzealous interpretation of territorial sovereignty is out of line with how similar situations are addressed in other areas of law. Consider, for example, a situation where a court in state A orders a company in state B to delete data that the company holds on a server in state B. In such situations, no one seems concerned about the implications for state B's territorial sovereignty. Yet, in this type of situation, the exercise of jurisdiction by state A is more severe, in that the data is actually deleted in state B, rather than merely accessed.

> "Several of the most recent initiatives in this field have moved past the traditional focus on territoriality"

It is, therefore, perhaps only natural that, as discussed further in Chapter 3.2.2.3, several of the most recent initiatives in this field have moved past the traditional focus on territoriality. The US CLOUD Act includes provisions that specifically disregard the location of data, and outlines obligations that apply "regardless of whether such communication, record, or other information is located within or outside of the United States"[375]. Similarly, both the aforementioned EU Regulation[376] and Directive[377] apply to service providers 'offering services' in the EU or a Member State, and neither the Regulation nor the Directive focuses on the location of the data in question.

The CLOUD Act explicitly recognizes that internet intermediaries may face situations in which compliance with a foreign government production order for data may necessitate the violation of US law, and vice versa. In light of this, the CLOUD Act includes provisions aimed at ensuring that a comity analysis is carried out in such situations.

Similarly, the EU Regulation and Directive include a rather sophisticated interest balancing as a clearly articulated aspect of these instruments – particularly in relation to Articles 15 and 16 of the Regulation. They aim to ensure comity with respect to the sovereign interests of third countries, to protect the individual concerned, and to address conflicting obligations on service providers by providing a mechanism for judicial review in cases of clashes with third states.[378] These provisions instruct the court to engage in an interest balancing exercise:

> "Weighing a number of elements which are designed to ascertain the strength of the connection to either of the two jurisdictions involved, the respective interests in obtaining or instead preventing disclosure of the data, and the possible consequences for the service provider of having to comply with the Order."[379]

---

375. Clarifying Lawful Overseas Use of Data Act S.2383. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

376. European Commission. (2018, April 17). *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.* COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

377. European Commission. (2018, April 17). *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.* COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.

378. European Commission. (2018, April 17). *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. COM(2018) 225 final*, Recital 47.

379. European Commission. (2018, April 17). *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. COM(2018) 225 final*, Recital 52.

3.2.3

Surveillance

The internet naturally lends itself to surveillance from both the public and private sector. The scale of state surveillance – both domestically and internationally – gained considerable attention in the wake of Edward Snowden's revelations in 2013, particularly those regarding the US PRISM surveillance program.[380] Yet, there are constantly reports of new surveillance initiatives. For example, on December 20, 2018, the Indian Government issued an order allowing ten public agencies to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer.[381] Individuals and organizations refusing to comply with requests to intercept, monitor or access citizens' data face up to seven years in prison.

In should also be noted that certain groups are at particular risk of surveillance. For example, journalists and civil rights advocates are frequently targeted.[382]

Further, there is a direct link between surveillance and data localization requirements. For example, on June 10, 2017, the New York Times reported on a proposed bill in the Egyptian Parliament that would require ride-sharing services like Uber and Dubai-based Careem to store users' data in the country's territory.[383] The Egyptian government reportedly justified the bill as necessary for fighting against terrorists, while NGOs like Privacy International have expressed concern that the law could be part of a broader surveillance effort.[384]

Several interviewed experts emphasized the Chinese 'social credit system' as a particularly invasive form of emerging surveillance. There is still considerable uncertainty as to how exactly the system will work when finalized.[385] However, in broad terms, social credit is like a personal scorecard for each of China's 1.4 billion citizens. The score is based on information gained from government records – including educational and medical, state security assessments and financial records – supplemented by constant surveillance via CCTV cameras and smartphone monitoring, as well as the tracking of internet browsing and shopping habits. The social credit score is also affected by the behavior of an individual's friends and family, as well as by whom they date.[386]

Citizens with a high score may enjoy benefits such as VIP treatment at hotels and airports, cheaper loans, and a fast track to the best schools, universities, health care and jobs. Those with low scores may be locked out of society and social media, and may be barred from travelling or receiving credit or government jobs.[387] Trials are being undertaken in a number of cities across China, and the ambition seems to be that by 2020, the system will be implemented nationally.[388] Yet, the Chinese government has yet to explain exactly how the social credit system will work, how the algorithmic credit scoring will be amassed and how the different qualities will be weighed against one another.[389]

While predominantly discussed as a domestic issue so far, the cross-border dimension of surveillance is likely to increase in prominence in coming years. For example, it may not be far-fetched to imagine the mentioned Chinese social credit system (1) being adopted in some form by other states either voluntarily or as part of broader agreements with China, and (2) being extended also to persons outside China so as to for example affect visa applications to China. In fact, in September 2019, it was reported that Chinese authorities want to collate information from both domestic and foreign businesses operating in China and integrate them into a centralized digital database aimed at establishing a credit record system for market players and institutions.[390]

---

380. Wikipedia. *PRISM (surveillance program)*. Retrieved from https://en.wikipedia.org/wiki/PRISM_(surveillance_program).

381. Internet & Jurisdiction Policy Network. (2018, December). India: Government issues order allowing agencies to intercept, monitor and decrypt user data. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7725_2018-12.

382. See e.g.: United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2019). Report of the Special Rapporteur to the Human Rights Council on surveillance and human rights. A/HRC/41/35. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement.

383. Walsh, D. (2017, June 10). Dilemma for Uber and Rival: Egypt's demand for data on riders. *The New York Times*. Retrieved from https://www.nytimes.com/2017/06/10/world/middleeast/egypt-uber-sisi-surveillance-repression-careem.html.

384. Internet & Jurisdiction Policy Network. (2017, June). Egyptian draft bill would introduce data localization rules for ride-sharing services. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6103_2017-06.

385. Matsakis, L. (2019, July 29). How the West got China's social credit system wrong. *Wired*. Retrieved from https://www.wired.com/story/china-social-credit-score-system/.

386. Carney, M. (2018, September 18). Leave no dark corner. *ABC News*. Retrieved from https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278.

387. Carney, M. (2018, September 18). Leave no dark corner. *ABC News*. Retrieved from https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278.

388. Hatton, C. (2015, October 26). China 'social credit': Beijing sets up huge system. *BBC News*. Retrieved from https://www.bbc.com/news/world-asia-china-34592186.

389. Liu, J. (2018, December 6). Is China's social credit system really the dystopian si-fi scenario that many fear? *Science Nordic*. Retrieved from http://sciencenordic.com/china's-social-credit-system-really-dystopian-si-fi-scenario-many-fear.

390. Cheng, E. (2019, September 3). China is building a 'comprehensive system' for tracking companies' activities, report says. *CNBC*. Retrieved from https://www.cnbc.com/2019/09/04/china-plans-for-corporate-social-credit-system-eu-sinolytics-report.html.

3.2.3.1 Data retention laws

The term data retention broadly refers to data being retained for a variety of purposes, including legal or business purposes. Here, however, the term is used in a narrower sense. The idea behind data retention laws is to ensure access to evidence by retaining all communications for later inspection, should a need arise.

This practice may give rise to cross-border legal challenges because data retention regimes will invariably capture large amounts of personal data on foreigners, for example, who are temporarily visiting the country or, potentially, on foreigners who communicate with people in that country. In other words, data retention laws in one state may impact the data privacy of internet users in other states.

Given the difficulty in predicting what data may be useful in the future, data retention schemes require the untargeted surveillance of *everyone*'s data. This has serious data privacy implications that frequently have a transnational dimension.

In light of these implications, data retention laws have sparked considerable controversy. The most prominent example of this occurred in 2014, when the CJEU declared the EU's Data Retention Directive (Directive 2006/24/EC) invalid for violating fundamental rights.[391] In response to this development, several EU Member States adopted new versions of data retention laws, and case law has continued to emerge on data retention laws. In Joined Cases C-203/15 and C-698/15, the CJEU noted that national data retention legislation "must make provision for the data to be retained within the European Union"[392] In this way, data retention laws may introduce mandatory data localization requirements. While these European disputes have gained by far the most international attention, data retention laws are widespread.

The type of data retention discussed above must be distinguished from the retention of specifically identified data, as is the case in situations where law enforcement requests a data holder to ensure the retention of specific data for a period required for the investigation. This latter form of data retention may play an important role in any structure under which law enforcement is encouraged to seek relevant data directly from the data owner, rather than from the internet intermediary that holds the data.

On October 2, 2018, the CJEU ruled[393] that national law enforcement authorities can access personal data held by telecommunication companies, as long as that access does not constitute a serious infringement of privacy.[394] In particular, the court argued that access to basic subscriber information, as necessary to investigate and prosecute minor criminal offenses, was justifiable. Furthermore, at the time of writing there are ongoing cases before the CJEU relating to data retention.[395]

Data retention laws are not limited to the EU. For example, on July 1, 2018 the so-called 'Yarovaya laws', which introduce requirements for Russian internet and telecommunication companies to store user correspondence for six months, entered into force in Russia.[396] The requirements only apply to companies listed on the register of information disseminators on the internet, which does not include foreign internet platforms.

---

391. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.

392. Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, para 122.

393. Court of Justice of the European Union. (2018, October 2). *Criminal offences that are not particularly serious may justify access to personal data retained by providers of electronic communications services provided that that access does not constitute a serious infringement of privacy*. [Press Release] Luxembourg. Retrieved from https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/10/CP180141EN-1.pdf.

394. Internet & Jurisdiction Policy Network. (2018, October). ECJ rules law enforcement can access personal data held by telecommunication operators if it does not seriously infringe on privacy. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7552_2018-10.

395. See: Case C-520/18**.** For the EU position, see also: Council of the European Union. (2019, June 6). *Data retention to fight crime: Council adopts conclusions*. [Press Release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/.

396. Internet & Jurisdiction Policy Network. (2018, July). Russian law requiring platform and telecommunication operators to retain user correspondence enters into force. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7186_2018-07.

3.2.3.2 Encryption and backdoors

On August 17, 2018, it was reported[397] that the US Department of Justice had asked Facebook to break the encryption in its Messenger app, in order for law enforcement officials to be able to listen to a suspect's voice conversations.[398] Such requests occur both domestically and across borders. Obvious jurisdictional issues arise in the latter situation, but domestic requests may also have transnational implications, as they can set precedents for requests by other states.

The refusal to adhere to state decryption may result in services being blocked in certain countries, as well. For example, on May 1, 2018, it was reported that Iran's judicial authorities had ordered the encrypted messaging service Telegram to be blocked in the country. Iran's judiciary justified the ban by stating that Telegram was used to promote propaganda against the establishment, encourage terrorist activities, spread lies to incite public opinion, spark anti-government protests and distribute pornography. On May 5, 2018, in a post on Instagram, Iran's President Hassan Rouhani criticized the ban, indicating that it was not originated by his government.[399]

There is a long-standing discussion about encryption, but it is mainly carried out on a national level. There is a clear need for greater cooperation and coordination on a transnational level.[400]

Concerns about the impact of encryption on law enforcement efficiency have been raised for some time. Encryption technologies are now cheap and widespread, and the encryption of communication and stored data is indisputably an obstacle for the detection, prevention and investigation of criminal activity. Absent further analysis, it may seem obvious to provide law enforcement with backdoors that allow decryption, or to even ban the encryption of communications and data altogether.

To see the problems with such simplistic approaches, one need only consider the extent to which our daily activities rely on the encryption of stored data and communications. Imagine doing online banking without encryption, or making a purchase online with an unencrypted credit card number. Imagine logging into your hotel booking site, airline miles program, or email account without your credentials being protected by encryption. In short, much of what we do online depends on encryption.

As repeatedly noted in the encryption debate, there is broad industry agreement that third-party access to encryption keys – such as law enforcement backdoors, or other mechanisms that undermine encryption – weakens encryption for all users, including those not targeted by the law enforcement agency. Despite this, the debate continues to be framed in overly simplistic terms.

In the aftermath of the 2015 mass shooting in San Bernardino, California, the Federal Bureau of Investigation (FBI) sought access to one of the offenders' password-protected iPhone 5C. The phone in question used iOS 8 operating system, which had advanced security features, including encryption. Apple claimed that it could not break the encryption without creating a backdoor, but the FBI wanted the company to alter the System Information File (SIF), which would facilitate circumvention of the phone's security features. Apple refused. This confrontation ended when the FBI managed to access the iPhone with third party assistance – reportedly from outside the US. However, this conclusion did little to resolve the important legal, ethical and technical, debate to which the case gave rise.

Second, as previously noted, Australia's controversial Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 received Royal Assent and became law in December 2018. The law has gained worldwide attention due to its far-reaching negative impact on encryption. For example, Access Now noted that:

> "The legislation would allow the Australian government to issue secret orders to compel companies and providers to do 'acts or things' to comply with lawful orders to provide information. That could mean guaranteeing access to otherwise secure messaging platforms like WhatsApp. [...] The impact that this will have on companies small and large cannot be enumerated. It will undoubtedly undermine user trust in their products and services not only in Australia but around the world."[401]

As alluded to in this quote, the central jurisdictional issue in the encryption debate stems from the fact that, as the same products are adopted by

---

397. Levine, D. & Menn, J. (2018, August 18). Exclusive: U.S. government seeks Facebook help to wiretap Messenger - sources. *Reuters*. Retrieved from https://www.reuters.com/article/us-facebook-encryption-exclusive/exclusive-u-s-government-seeks-facebook-help-to-wiretap-messenger-sources-idUSKBN1L226D.

398. Internet & Jurisdiction Policy Network. (2018, August). US DOJ reportedly asks Facebook to break Messenger's encryption in criminal investigation. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7248_2018-08.

399. Internet & Jurisdiction Policy Network. (2018, May). Iran blocks encrypted messaging service Telegram. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7040_2018-05.

400. For one such initiative see: The Carnegie Endowment for International Peace. *Encryption Working Group*. Retrieved from https://carnegieendowment.org/programs/technology/cyber/encryption.

401. Access Now. (2018, December 6). *Australia joins Russia and China in undermining users' security and threatening human rights*. Retrieved from https://www.accessnow.org/australia-joins-russia-and-china-in-undermining-users-security-and-threatening-human-rights/.

users in multiple countries, if one state takes steps to undermine the encryption used in those products, it effectively weakens encryption for users in all states in which the product is used.

There are also many parallels between the jurisdictional and procedural issues that arise in situations where law enforcement agencies seek access to data held by private parties, such as internet intermediaries (discussed above in Chapter 3.2.2), and those that arise in the context of encryption and backdoors.

Considering the above, we can expect the debate about encryption to persist for the foreseeable future, and for more initiatives to appear. On October 6, 2017, for example, the prosecution offices of France, Belgium, Spain and Morocco released a common declaration expressing their desire for legislations to allow judicial authorities, with respect to strict procedural guarantees, to have access to encrypted data when lives are at stake, such as in the case of terrorism.[402] In July 2019, the Five Eyes Security Alliance of US, UK, Australia, Canada and New Zealand reportedly also called on tech companies to allow law enforcement to access encrypted material.[403]

> "The central jurisdictional issue in the encryption debate stems from the fact that, as the same products are adopted by users in multiple countries, if one state takes steps to undermining the encryption used in those products, it effectively weakens encryption for users in all states in which the product is used."

3.2.4

Cybersecurity

Work on ensuring an adequate degree of cyber security is typically conducted on a national level. This is natural considering the strong link, and indeed overlap, between cybersecurity and national security. At the same time, though, given that cybersecurity threats often originate from abroad and that several states may be affected by the same cyber threat, the international dimension is undeniable,[404] and international cooperation is both natural and necessary. The need for international cooperation is augmented by the degree to which states use hardware and software originating in other states.

Some examples of international cooperation include:

The **Asia-Pacific Computer Emergency Response Team** (APCERT), which is a group of leading and national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams dedicated to the protection of national infrastructure in the Asia-Pacific. Further, the ASEAN region is increasingly coordinating its efforts to reinforce regional cybersecurity.[405]

In **December 2018**, the **European Parliament**, **the Council and the European Commission** reached a political agreement on the EU Cybersecurity Act.[406] That Act is now in force.[407] Further, the EU's Directive on security of network and information systems (the NIS Directive) entered into force in **August 2016**.[408] Member States had to transpose the Directive into their national laws by **9 May 2018**.

---

402. Koen Geens Ministre de la Justice. (2017, October 4). *Quadripartite Maroc / Espagne / France / Belgique.* Retrieved from https://www.koengeens.be/fr/news/2017/10/04/quadripartite-maroc-espagne-france-belgique-1.

403. Hosenball, M. & Holden, M. (2019, July 30). 'Five Eyes' security alliance calls for access to encrypted material. *Reuters.* Retrieved from https://www.reuters.com/article/us-security-fiveeyes-britain/five-eyes-security-alliance-calls-for-access-to-encrypted-material-idUSKCN1UP199.

404. See further: Kettemann, M. (2019) "This is not a drill": International law and protection of cybersecurity, in Wagner/Kettemann/Vieth (eds.), *Research Handbook of Human Rights and Digital Technology*. Cheltenham, Edward Elgar.

405. Thomas, J. (2019, August 3). Intensifying ASEAN's cybersecurity efforts. *The ASEAN Post*. Retrieved from https://theaseanpost.com/article/intensifying-aseans-cybersecurity-efforts; ASEAN. (2017, December 1). *ASEAN Telecommunications and Information Technology Ministers.* [Joint Media Statement]. Siem Reap, Cambodia. Retrieved from https://asean.org/wp-content/uploads/2012/05/14-TELMIN-17-JMS_adopted.pdf; ASEAN-United States leaders' statement on cybersecurity cooperation. (2018). Retrieved from https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf. Baharudin, H. (2018, September 20). ASEAN framework on cyber security in the works. *Straits Times.* Retrieved from https://www.straitstimes.com/singapore/asean-framework-on-cyber-security-in-the-works.

406. European Commission. (2018, December 11). *EU negotiators agree on strengthening Europe's cybersecurity*. Retrieved from https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

407. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

408. European Commission. (2019). *The Directive on security of network and information systems (NIS Directive).* Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

Mutually Agreed Norms for Routing Security (MANRS), a global initiative supported by the Internet Society. It provides crucial fixes to reduce the most common routing threats; in **December 2018**, the number of network operators that have agreed to MANRS surpassed 100.[409]

In **June 2018**, the **Global Partners Digital** published its report titled Multistakeholder Approaches to National Cybersecurity Strategy Development.[410]

At the **2018** Internet Governance Forum, **French** President Macron launched the Paris Call for Trust and Security in Cyberspace.[411]

The **United Nations Group of Governmental Experts** (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security has been working for some time on norm setting in cyberspace.[412]

The **Global Commission on the Stability of Cyberspace**, which seeks to set consistent norms related to the security and stability of cyberspace.[413]

Led by Russia and China, the members states of the **Shanghai Cooperation Organisation** (SCO) are pursuing the development of universal international norms, rules and principles concerning responsible behavior of states in the information space: "Specifically, in **2015** China distributed an updated version of the Rules of Conduct in the Field of International Information Security on behalf of the SCO member states as an official UN document."[414]

The **Organization for Security and Co-operation in Europe** has undertaken work, organized events,[415] and issued Decisions in the field of cybersecurity.[416]

The **Cybersecurity Initiative by New America**, which aims to build an International Cyber Network to publish on cybersecurity issues.[417]

The **Carnegie Endowment for International Peace** carries out a range of initiatives in the cybersecurity sphere.[418]

---

409. Mutually Agreed Norms for Routing Security. Retrieved from https://www.manrs.org/.
410. Schnidrig, D. & Kaspar, L. (2018, June 27). Multistakeholder approaches to national cybersecurity development. *Global Partners Digital*. Retrieved from https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/.
411. Paris call for trust and security in cyberspace. (2018, November 12). Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.
412. See e.g.: Roigas, H. & Minarik, T. (2015). 2015 UN GGE Report: Major players recommending norms of behavior, highlighting aspects of international law. *NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/: and Grigsby, A. (2018, November 15). The United Nations doubles its workload on cyber norms, and not everyone is pleased. *Council of Foreign Relations*. Retrieved from https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
413. Global Commission on the Stability of Cyberspace. (2018). Retrieved from https://cyberstability.org/about/.
414. Shanghai Cooperation Organisation. (2019, May 16). *SCO participation at the 4th Central Asian Internet Governance Forum: Internet for Increasing capacities in central Asia*. Retrieved from http://eng.sectsco.org/news/20190516/540999.html.
415. Organization for Security and Cooperation in Europe. (2019, June 19). *Officials, practitioners and experts gather in Bratislava for OSCE-wide conference on the future of cybersecurity*. [Press Release]. Bratislava. Retrieved from https://www.osce.org/chairmanship/423365.
416. See e.g. Organization for Security and Cooperation in Europe. (2016, March 10). *Decision No, 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. PC.DEC/1202. Retrieved from https://www.osce.org/pc/227281?download=true.
417. New America. *Cybersecurity initiative*. Retrieved from https://www.newamerica.org/cybersecurity-initiative/about/.
418. See e.g.: Carnegie Endowment for International Peace. *Cyber strategy*. Retrieved from https://carnegieendowment.org/programs/technology/cyber/cyberstrategy/; Carnegie Endowment for International Peace. *Cybersecurity and the financial system*. Retrieved from https://carnegieendowment.org/specialprojects/fincyber; Carnegie Endowment for International Peace. *U.S.-China cyber stability*. Retrieved from https://carnegieendowment.org/programs/technology/cyber/uschinacyberstability; Carnegie Endowment for International Peace. *International cybersecurity norms*. Retrieved from https://carnegieendowment.org/specialprojects/cybernorms/?lang=en.

At the same time, international cooperation should not be unconditional merely because it falls under the banner of cyber security, or indeed cybercrime. For example, China's *Cybersecurity Law* became effective in June 2017, and speculations that the law would be used extensively for political purposes have thus far proven true: "Since the law took effect, over 40 percent of the enforcement actions were to remove 'politically harmful contents,' and less than 3 percent were for protecting the 'rights and interests of the 'internet user.'"[419] Thailand's recently approved *Cybersecurity Law* is also controversial with some reported concerns about provisions permitting the government access to user data in a "national emergency".[420] Observers who have followed the law's development closely have warned that, while the law is driven by good intentions it overreaches in several respects.[421]

This is part of a broader concern about international mechanisms for law enforcement cooperation being abused for the purpose of politically motivated persecution of dissidents. A December 2018 POLITICO article, for example, outlines how "the international policing system has already been hijacked by autocrats like Russian President Vladimir Putin who are using it to crack down on their critics and have powerful Western allies to help them."[422] The need for appropriate due process safeguards cannot be overstated.

Furthermore, cybersecurity considerations are often the source of forced data localization requirements (discussed further in Chapter 4.2.7), and sometimes of 'rep localization' requirements, as well (discussed further in Chapter 4.1.3). For example, on November 2, 2018, the Vietnamese government released a draft decree on guidelines to implement its Law on Cybersecurity No. 24/2018/QH14 ('the Cybersecurity Law'), which was approved on June 12, 2018. The law requires service providers to establish a local office and comply with data localization requirements.[423] On February 24, 2018, it was reported that Apple would begin storing Chinese iCloud accounts and encryption keys in China from February 28, 2018, marking a change in its previous policy of only storing encryption keys in the US.[424] The decision to store Chinese iCloud data on servers owned and operated by state-run Chinese company Guizhou-Cloud Big Data (GCBD) was explained as being necessary to comply with a data localization requirement in the country's Cybersecurity Law, introduced on June 1, 2017.[425]

The internet was not constructed with security in mind. In that sense, cyber security is always going to be an afterthought, unless the internet is fundamentally changed. On the positive side, however, there is undoubtedly an increasing awareness of the risks involved, and that awareness is translating into greater preparedness to address those risks. For example, on 9 October 2019, the EU released a risk assessment of 5G networks security.[426] Nevertheless, the scale and severity of the cybersecurity challenge should not be understated. The immediate future, at least, appears rather gloomy, with no end in sight to the constant 'cat-and-mouse game' between attackers and those seeking to ensure cybersecurity.

In this context, one interviewed expert made the point that infrastructure originally set up by criminals for criminal activities is now being adopted by state-sponsored activities aimed at, for example, election fraud, fake news and hate speech. This, the expert stressed, is a major challenge for the cybersecurity industry.

> "The need for appropriate due process safeguards cannot be overstated."

---

419. The National Law Review. (2018, January 9). *Top data governance issues from 2017 and what to watch in 2018*. Retrieved from https://www.natlawreview.com/article/top-data-governance-issues-2017-and-what-to-watch-2018.

420. Tech Crunch. (2019, February 28). *Thailand passes controversial cybersecurity law that could enable government surveillance*. Retrieved from https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/.

421. Leesa-Nguansuk, S. Tortermvasana, K. & Banchongduang, S. (2018, October 22). The cybersecurity balancing act. *Bangkok Post*. Retrieved from https://www.bangkokpost.com/thailand/politics/1562230/the-cybersecurity-balancing-act.

422. Eristavi, M. (2018, December 13). Interpol keeps despots' dissidents close. *Politico*. Retrieved from https://www.politico.eu/article/interpol-russian-abuse-keeps-despots-dissidents-close/.

423. Internet & Jurisdiction Policy Network. (2018, November). Vietnamese government releases draft decree on implementation of cybersecurity law requiring service providers to establish local offices, store data within the country. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7691_2018-11.

424. Nellis, S. & Cadell, C. (2018, February 24). Apple moves to store iCloud keys in China, raising human rights fears. *Reuters*. Retrieved from https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060.

425. Internet & Jurisdiction Policy Network. (2018, February). Apple stores Chinese iCloud accounts and encryption keys in China to comply with data localization requirements. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6817_2018-02.

426. European Commission NIS Cooperation Group. (2019). *Report: EU coordinated risk assessment of the cybersecurity of 5G networks*. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

3.2.4.1 Data breaches – a modern trans-border plague

In 2017, a major data breach at Equifax affected more than 100 million credit users worldwide, underscoring global implications that are relevant to cross-border legal challenges online. With user data flowing across borders, the impact of a data breach in one country is rarely contained to that country. Users around the globe are affected, making it difficult for people to know whether their data has been leaked. Data breaches often involve the data of data subjects in multiple states, resulting in complex jurisdictional issues.

> "With user data flowing across borders, the impact of a data breach in one country is rarely contained to that country."

Data breaches occur for a variety of reasons. Systems could be hacked, as discussed below, or human error could be at fault. In December 2018, for instance, it was reported that a German user of Amazon's Alexa voice assistant "got access to more than a thousand recordings from another user because of a human error by the company."[427] Examples like this are commonly reported, and it is reasonable to suspect that numerous other incidents go unreported. These examples also illustrate the fact that small errors can have huge implications.

Other data breaches may arise in situations where individuals feel that the public deserves to know about confidential data. The many publications of leaked data on sites such as WikiLeaks fall into this category.

3.2.4.2 Hacking – a constant multilevel threat

As with most criminals, those who engage in hacking – whatever the purpose – may benefit from the cross-border legal challenges on the internet insofar as jurisdictional boundaries may impede effective detection, prevention, investigation and prosecution. As a result, successful prosecution is rare. Nevertheless, cross-border charges are sometimes filed, as when the US indicted a group of Chinese hackers who had "conspired to steal sensitive commercial technological, aviation, and aerospace data by hacking into computers in the United States and abroad."[428]

Hacking is carried out for a range of different reasons, ranging from financial reasons and curiosity to terrorism and military purposes. As emphasized earlier, it is often difficult to distinguish between civil and military hacking, due, in part, to difficulties in ensuring accurate attribution. Attackers often target the weakest points of a system, as well. For example, attempts to infiltrate national security and defense structures often target the networks of defense-affiliated organizations such as commercial contractors, rather than directly targeting government networks, which are typically more secure.[429]

As noted in a recent report, cyber espionage poses the most advanced threat to the private sector, and is carried out for a variety of reasons; "while it is generally associated with the theft of intellectual property, cyber espionage may also include the theft of other commercially sensitive information such as company negotiation strategies or business plans."[430]

3.2.4.3 Foreign storage of e-government data

The move toward e-government solutions gives rise to the same types of cybersecurity issues that arise in e-commerce. But while the provider of an e-commerce website may suffer financially if the website becomes unavailable, the outage of e-government solutions may risk paralyzing society. This places particularly high cyber security requirements on e-government solutions.

In addition, e-government solutions must be structured in a sufficiently robust manner to allow a government to continue operating in a state of emergency, including during an invasion by a foreign power. For example, Estonia – which has been a pioneer in the e-government sphere – has stated that to "support the Estonian 'digital' independence and uninterrupted operation of public IT services in state of emergency there is a long-term plan to establish e-embassies out-

---

427. Schuetze, A. (2018, December 20). Amazon error allowed Alexa user to eavesdrop on another home. *Reuters*. Retrieved from https://www.reuters.com/article/us-amazon-data-security-idUSKCN1OJ15J.

428. United States of America v Zhang et al 13CR3132-H, Indictment. Retrieved from https://www.justice.gov/opa/press-release/file/1106491/download, para 1.

429. Australian Cyber Security Centre. (2017). *Australian Cyber Security Centre 2017 Threat Report*. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf, p. 51.

430. Australian Cyber Security Centre. (2017). *Australian Cyber Security Centre 2017 Threat Report*. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf, p. 55.

side Estonia in friendly foreign countries."[431] Estonia and Luxembourg have reached an agreement under which Luxembourg will host an Estonian 'data embassy', which will have the same protection and immunity as traditional embassies.[432]

This type of agreement is likely to become more common, and it gives rise to complex jurisdictional considerations. In the case of disputes, for instance, data stored abroad may become subject to jurisdictional claims by the host state. Nevertheless, the arrangement is an interesting example of 'reverse extraterritoriality'; in effect, Luxembourg cedes certain rights it otherwise would hold over the territory on which the 'data embassy' is constructed.

3.3

Economy

In the economic coat the cross-border application of territorially based intellectual property rights, taxation, and emerging technologies such as the Internet of Things and blockchain. In the context of expression and security, as discussed above, the role of internet intermediaries is being re-examined. In fact, with regard to the economy, there seems to be a more profound change in attitudes toward internet platforms.

Although it was not always the case, economical activities are now a natural and important part of the online environment. For example, it has been estimated that at least half of all trade in services is supplied via the internet[433]; and the World Economic Forum has estimated that the overall economic value of digital transformation to business and society will exceed 100 trillion US dollars by 2025.[434] Indeed, even when offered free of monetary charges, most online uses and activities are commercial to a significant extent due to the 'data economy'.

The significance of the internet's economic dimension will continue to increase over the coming years, due to what has been termed Industry 4.0. That is:

> "the next phase in the digitization of the manufacturing sector, driven by four disruptions: the astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks; the emergence of analytics and business-intelligence capabilities; new forms of human-machine interaction such as touch interfaces and augmented-reality systems; and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing."[435]

The digitalization of the economy – via access to an open internet and constant technological developments – is a driving force for growth. It enables companies, and particularly SMEs, to compete on the world stage and create new opportunities in developing, ordering, producing, marketing or delivering their products and services. However, the ability to reach customers all over the globe at a faster pace and lower cost than ever before remains dependent upon a manageable regulatory environment.

"The ability to reach customers all over the globe at a faster pace and lower cost than ever before remains dependent upon a manageable regulatory environment."

Several surveyed and interviewed experts emphasized that complying with often complex laws from multi-

431. E-Estonia. *E-governance*. Retrieved from https://e-estonia.com/solutions/e-governance/.
432. Digital Luxembourg. *Data Embassy*. Retrieved from https://digital-luxembourg.public.lu/initiatives/data-embassy.
433. Lee-Makiyama. (2017, July 10). The digital trade oversight. *International Trade Forum*. Retrieved from http://www.tradeforum.org/article/The-digital-trade-oversight/.
434. Cann, O. (2016, January 22). $100 trillion by 2025: The digital dividend for society and business. *World Economic Forum*. Retrieved from https://www.weforum.org/press/2016/01/100-trillion-by-2025-the-digital-dividend-for-society-and-business/.
435. Baur, C. & Wee, D. (2015, June). Manufacturing's next act. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act.

ple sources calls for a degree of legal sophistication that is often beyond the reach of SMEs. Experts cited the complexity of privacy and consumer protection regulation and tax implications as specific examples. It was also noted that start-ups are exposed to the regulatory burden at a stage where they least can afford it. To build a user base, new businesses must often begin by giving away their services, before building a proven user base to secure revenue through advertisements. Yet, the cost of ensuring regulatory compliance is incurred from the start – indeed, even prior to the launch of the service.

Experts also noted that SMEs are too often not part of regulatory discussions, which largely focus on the internet giants. At the same time, some experts pointed out that, compared to the large internet actors, SMEs are better placed to ignore claims of jurisdiction from distant states, as they can more easily avoid placing persons and assets within the reach of those states' enforcement powers.

Cross-border legal challenges on the internet is a significant barrier for Small and Medium Enterprises (SMEs)

69% of surveyed experts 'agreed', or 'strongly agreed', that the complexity of cross-border legal challenges on the internet is a significant barrier for SMEs entering the global digital economy. 21% 'neither agreed nor disagreed', and only 10% either 'disagreed', or 'strongly disagreed'.

These figures were largely consistent across the different regions and stakeholder groups. Some, however, asserted that the complexity of cross-border legal challenges on the internet is not so much a barrier for SMEs *entering* the global digital economy, as it is a barrier for SMEs *seeking growth* in the global digital economy.

> "Cross-border trade on the internet also has the potential to be an equalizer between the developed and developing world."

Cross-border trade on the internet also has the potential to be an equalizer between the developed and developing world, as it allows developing countries to bypass some of the steps today's developed countries had to go through. Yet, while the potential advantages are great, so are some of the obstacles.

Cross-border legal challenges on the internet are a significant barrier for developing countries

In the survey study, 54% of surveyed experts 'agreed', or 'strongly agreed', that the complexity of cross-border legal challenges on the internet is a significant barrier for developing countries entering the global digital economy. 37.5% 'neither agreed nor disagreed', and only 8.5% either 'disagreed', or 'strongly disagreed', that the complexity of cross-border legal challenges on the internet is a significant barrier for developing countries entering the global digital economy.

One surveyed expert noted that even the fear of the legal difficulties associated with cross-border internet activity dissuades people in developing countries from engaging in such activities. Further, one interviewed expert noted that the main difficulty facing developing countries is the significantly faster pace at which the internet evolves today, compared to the past. The pace of change in the regulatory environment and its complexification – due, in large part, to an increased regulatory appetite and extraterritoriality – is increasing, as well. However, the survey also revealed a marked difference in attitudes among surveyed experts from different regions. Both surveyed and interviewed experts emphasized that poverty, skill levels, illiteracy, language barriers, political instability, lack of investors and poor ICT infrastructure are bigger concerns in regions such as Africa and some parts of Latin America, than are the legal cross-border challenges. Surveyed and interviewed experts also observed that much of the online activity in developing countries is local in nature, and therefore, confronts the complexity of cross-border legal challenges on the internet less often.

Experts also raised the point that developing countries are often not part of, and indeed not even aware of, agreements and other regulatory developments discussed or concluded among developed countries. Experts observed that developing countries experience difficulties when seeking to apply their laws in an extraterritorial manner that affects developing countries, including businesses and persons in developing countries. There is also a perception that, compared to developed countries, developing countries have less of a say in the approaches taken by major internet actors. This sense of disempowerment is a clear trend, and arguably pressures developing countries to choose between existing, partially competing approaches (e.g., between a 'Western approach' promoting democratic values and a Chinese 'digital sovereignty' approach) rather than having the opportunity to develop their own approaches.

Taken together, this suggests that although the complexity of cross-border legal challenges on the internet is an important barrier for developing countries entering the global digital economy, it is just one of several – and perhaps not the most acute. Yet, there is no doubt that, once the more pressing challenges have been addressed, the full impact of the cross-border legal challenges will inevitably be felt, unless they can be alleviated in advance.

In addition to what is discussed below, numerous other initiatives and developments should be noted:

In **July 2019, the Hague Conference on Private International Law** concluded its Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters (the Judgments Project).[436] Although it is too early to assess its implications, this is clearly an instrument of tremendous potential. In addition, the Hague Conference's 2015 Principles on Choice of Law in International Commercial Contracts,[437] and 2005 Convention on Choice of Court Agreements[438] are of direct relevance for online commerce.

APEC has launched a project aimed at identifying global trends in digital trade as well as opportunities and challenges to enabling SMEs to harness and benefit from digital trade. The project will also make recommendations to APEC on how to help SMEs take advantages of opportunities brought about by digital trade,[439] and a report was published in **June 2019**.[440]

In **July 2018**, the **UN** Secretary-General convened a High-Level Panel on Digital Cooperation. The outcome will be a report that aims to raise awareness on the impact of digital technologies on the economy and society, and present proposals for improvements to cooperation.[441]

The **UN Conference on Trade and Development** (UNCTAD) has demonstrated that **145 countries** (of which 104 are classed as developing or transition economies) have enacted e-transaction laws that recognize the legal equivalence between paper-based and electronic forms of exchange.[442]

The **World Economic Forum** is pursuing a variety of projects, such as its Digital Transformation Initiative, which aims to provide a base of evidence and a common language for public-private collaboration focused on ensuring that the benefits of digital transformation are fairly and widely shared.[443] Its Digital Trade Project supports the development of policy frameworks that maximize the benefits of digital trade and data flows.[444] In **2017**, the World Economic Forum published a white paper titled Making Deals in Cyberspace: What's the Problem?, which aims to build the knowledge of current e-transaction and e-signature rules.[445] That paper concluded that: "While many countries already have baseline e-transaction laws in place […]divergences in details are manifest and do not always address cross-border aspects."[446]

---

436. Hague Conference on Private International Law. (2019, July 2). *Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters*. Retrieved from https://www.hcch.net/en/instruments/conventions/full-text/?cid=137.
437. Hague Conference on Private International Law. (2015, March 19). *Principles on choice of law in international commercial contracts*. Retrieved from https://www.hcch.net/en/instruments/conventions/full-text/?cid=135.
438. Hague Conference on Private International Law. Hague *Convention of 30 June 2005 on choice of court agreements*. Retrieved from https://www.hcch.net/en/instruments/conventions/specialised-sections/choice-of-court.
439. Asia-Pacific Economic Cooperation. *APEC workshop on harnessing digital trade for SMEs*. Retrieved from https://aimp2.apec.org/sites/PDB/Lists/Proposals/DispForm.aspx?ID=2252.
440. Asia-Pacific Economic Cooperation. *APEC Workshop on Harnessing Digital Trade for SMEs*. Retrieved from https://www.apec.org/-/media/APEC/Publications/2019/6/APEC-Workshop-on-Harnessing-Digital-Trade-for-SMEs/219_SME_APEC-Workshop-on-Harnessing-Digital-Trade-for-SMEs.pdf.
441. United Nations. (2018). *Secretary-General's High-level Panel on Digital Cooperation*. Retrieved from http://www.un.org/en/digital-cooperation-panel/.
442. United Nations Conference on Trade and Development. *E-transactions legislation worldwide*. Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Transactions-Laws.aspx.
443. World Economic Forum. (2018, May). *Digital Transformation Initiative*. Retrieved from http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-executive-summary-20180510.pdf.
444. World Economic Forum. *Digital Trade*. Retrieved from https://www.weforum.org/projects/digital-trade-policy.
445. World Economic Forum. (2017, October). *White Paper: Making deals in cyberspace: What's the problem?* Retrieved from http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf.
446. World Economic Forum. (2017, October). *White Paper: Making deals in cyberspace: What's the problem?* Retrieved from http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf, at 11.

At the **G20** meeting in Düsseldorf, Germany in **2017**, the Ministers with responsibility for the digital economy issued the G20 Digital Economy Ministerial Declaration (or the Dusseldorf Declaration), which includes a Roadmap for Digitization setting out policies for the digital economy and the G20 Priorities on Digital Trade.[447]

In **2017**, the **OECD** released its biennial report on emerging challenges and opportunities for the digital economy: the OECD Digital Economy Outlook 2017.[448] The OECD has also established an Advisory Group on Measuring GDP in a Digitalized Economy.[449]

The **World Economic Forum** is also involved in a joint Enabling E-Commerce Initiative with the **World Trade Organization** and the **Electronic World Trade Platform**. The initiative seeks to encourage high-level discussions on how e-commerce policies can benefit SMEs.[450]

The **Global Forum on Cyber Expertise** considers what countries, international organizations and private companies can do to exchange best practices and initiatives on cyber capacity building.[451] The **International Telecommunications Union** (ITU) has similarly considered capacity building for the digital economy.[452]

The **World Trade Organization** (WTO) engages with the digital economy from a variety of angles. As early as **1998**, the WTO recognized that global electronic commerce was growing and creating new opportunities for trade, and it responded by adopting its Declaration on Global Electronic Commerce.[453] Several other initiatives may be noted,[454] as well. The Doha Declaration endorsed the work already done on electronic commerce, and instructed the General Council to consider the most appropriate institutional arrangements for handling the work program, and to report on further progress to the Fifth Ministerial Conference.[455]

Since the **mid-1990s**, the **United Nations Commission on International Trade Law** (UNCITRAL) has worked to increase the uniformity of laws governing e-transactions, e-signatures and digital authentication. Its key achievements are: (1) UNCITRAL Model Law on Electronic Commerce (MLEC) (1996), (2) UNCITRAL Model Law on Electronic Signatures (MLES) (2001), (3) United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) (2005), and (4) UNCITRAL Model Law on Electronic Transferable Records (MLETR) (2017).

---

447. *G20 Digital Economy Ministerial Declaration: Shaping digitalisation for an interconnected world.* (2017, April 7), Dusseldorf. Retrieved from http://www.g20.utoronto.ca/2017/170407-digitalization.html.
448. OECD. (2017). *OECD Digital Economy Outlook 2017*. Paris: OECD Publishing. Retrieved from https://read.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#page1.
449. Ahmad, N. & Ribarsky, J. (2018, September). *Towards a framework for measuring the digital economy, OECD*. Paper prepared for the 16th Conference of the International Association of Official Statisticians, France. Retrieved from http://www.oecd.org/iaos2018/programme/IAOS-OECD2018_Ahmad-Ribarsky.pdf.
450. World Economic Forum. (2017, December 11). *WTO, World Economic Forum and eWTP launch joint public-private dialogue to open up e-commerce for small business*. Retrieved from https://www.weforum.org/press/2017/12/trade-press-release/.
451. Global Forum on Cyber Expertise. (2019). Retrieved from https://www.thegfce.com.
452. International Telecommunications Union. (2018). *Developing skills for the digital economy and society*. Retrieved from https://www.itu.int/en/itunews/Documents/2018/2018-ITUNewsPlus-CBS/2017_ITUNewsPlus-CBS.pdf.
453. World Trade Organization. (1998, May 25). *The Geneva Ministerial Declaration on global electronic commerce*. Retrieved from https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm.
454. World Trade Organization. *Electronic commerce*. Retrieved from https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.
455. World Trade Organization. *The Doha Declaration explained*. Retrieved from https://www.wto.org/english/tratop_e/dda_e/dohaexplained_e.htm#electroniccommerce.

3.3.1

Intellectual property

Several cross-border legal challenges on the internet relate to intellectual property issues. A 2013 study by the Fordham Center on Law and Information Policy found that a majority of the seminal internet jurisdiction cases in the US centered on disputes regarding intellectual property. Of those cases, 43% related to trademarks, 20% related to copyright and 9% related to patents.[456]

The field of intellectual property has sparked many of the earliest internet jurisdiction cases, including the well-known *Zippo* case,[457] in which the Court devised the famous 'sliding scale' test (see Chapter 2.2.5), and cross-border intellectual property matters continue to generate challenges today. These challenges relate, for example, to obstacles for effective enforcement of intellectual property rights, the balancing of such rights against other rights (e.g., data privacy and freedom of expression), and scope of jurisdiction issues such as those that came before the Supreme Court of Canada in the *Equustek* case.[458] In that case, the court reaffirmed the injunction from a British Columbia judge forcing Google to remove search results globally, rather than just within the Canadian territory,[459] but the dispute continued well beyond the Supreme Court of Canada's June 2017 decision.[460] As recently as April 2018, the Supreme Court of British Columbia, Canada issued a decision denying Google's request to change an injunction requiring it to delist search engine results globally in the *Equustek* case.[461] Moreover, the role of internet intermediaries in preventing, detecting, investigating, and taking legal action in response to intellectual property infringements has gained considerable attention – in addition to questions of their liability. Indeed, there are several recent examples of this attention, including the German Federal Court of Justice's decision, in September 2018, to refer a case to the CJEU over whether YouTube can be held liable for hosting copyright-infringing videos.[462] In some jurisdictions, the courts have determined that providers are not liable for infringing content. For example, the Swiss Supreme Court recently ruled that internet service providers could not be required to block websites that include copyright-infringing movies.[463] Also, the Austrian Appeals Court overturned a previous decision to find YouTube not liable for copyright-infringing material on the basis that YouTube does not have an 'active role' in copyright infringement.[464] In other jurisdictions, courts have held video sharing platforms (in Italy) and media organizations (in Australia) to be liable for the content uploaded by users.[465] Indian courts have found that the question of whether an e-commerce platform is an 'intermediary' (and therefore, protected by safe harbor provisions in Indian law), depends on whether they played only an inactive or passive role in the marketing and selling process. In the case of *Christian Louboutin SAS vs Nakul Bajaj and Ors*,[466] the platform was held

---

456. Reidenberg, J.R., Debelak, J., Kovnot, J., Bright, M., Russell, N.C. Alvarado, D., Seiderman, E. & Rosen, A. (2013, June 30). Internet jurisdiction: A survey of legal scholarship published in English and United States case law. *Fordham Law Legal Studies Research Paper No. 2309526*. Retrieved from SSRN http://ssrn.com/abstract=2309526 or http://dx.doi.org/10.2139/ssrn.2309526, at 56-57 (footnotes omitted).

457. Zippo Manufacturing Company v Zippo Dot Com, Inc. 952 F.Supp. 1119 (W.D.Pa 1997).

458. Google Inc v Equustek Solutions Inc 2017 SCC 34.

459. Google Inc v Equustek Solutions Inc 2017 SCC 34. Retrieved from https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

460. Geist, M. (2017, November 3). *U.S. Judge Rules Canadian court order 'threatens free speech on the global internet'*. Retrieved from http://www.michaelgeist.ca/2017/11/googleequustekinjunction/.

461. Internet & Jurisdiction Policy Network. (2018, April). Canada: Regional court upholds Equustek decision requiring Google to globally delist search results in spite of US court decision. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6957_2018-04.

462. Internet & Jurisdiction Policy Network. (2018, September). Highest German court refers case on YouTube liability over copyright-infringing videos to ECJ. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7454_2018-09. See further: Case C-682/18 LF v Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=211267&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1142050.

463. Geigner, T. (2019, March 6). Swiss Supreme Court refuses to order ISPs to block 'pirate' sites. *Tech Dirt*. Retrieved from https://www.techdirt.com/articles/20190228/11582441695/swiss-supreme-court-refuses-to-order-isps-to-block-pirate-sites.shtml.

464. Torrent Freak. (2019, March 13). *YouTube is not liable for copyright infringing videos, Appeal Court rules*. Retrieved from https://torrentfreak.com/youtube-is-not-liable-for-copyright-infringing-videos-appeal-court-rules-190312/.

465. Internet & Jurisdiction Policy Network. (2019, July). Italian court holds video sharing platform liable for content uploaded by users. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaXRhbGlhbiIsImZyb20iOiIyMDEyLTAyIiwidG8iOiIyMDE5LTA4In0=; Internet & Jurisdiction Policy Network. (2019, June). Australian court rules media organizations liable for content posted by users on their pages. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiYXVzdHJhbGlhIiwiZnJvbSI6IjIwMTItMDliLCJ0byI6IjIwMTktMDgifQ==.

466. CS(COMM) 344/2018.

to be liable as taking an active role in the marketing and sale of infringing products.[467] An additional initiative is the proposed amendments to Russia's copyright law, which would allow rights-holders to order web hosts to block sites with pirated material without a court application if there is no response to take-down requests.[468]

The frequency with which internet jurisdiction issues arise in the context of intellectual property may not be surprising given the contrast between the strongly territorial nature of intellectual property rights, on the one hand, and the global nature of the internet, on the other. As pointed out by one surveyed expert, trademark rights are determined and limited by each jurisdiction, which establishes, within its own territorial limits, the prerequisites for trademark protection and the standards for infringement and defenses, such as when a trademark cannot be a basis for excluding others from using it, for example, as functional, fair use, or generic. A trademark may, therefore, be valid or famous in one jurisdiction, but not in another. Enabling one jurisdiction to determine the global enforceability of a trademark is thus at odds with the territorial basis of trademark rights.

At the same time, it has been observed that intellectual property rights "cannot be linked to a precise physical and geographical territory, but rather are social and universal phenomena."[469] And that the "risk of transnational misappropriation of IPRs raises a number of issues of how to protect these rights universally, exposing the territorial principle to increasing doubts."[470]

Within this context, several initiatives should be noted:

The **EU** Directive on Copyright in the Digital Single Market[471] (2018 EU Copyright Directive) was adopted by the European Parliament in **March 2019**[472] and is designed to update copyright laws for the digital environment. Article 13 of the proposed directive controversially requires websites such as YouTube, Google and Facebook to take 'appropriate and proportionate' measures to prevent users posting unauthorized copyright content (known as the filtering measure or, by some critics, the meme ban). As far as the EU is concerned, attention should also be directed at the Directive on the enforcement of intellectual property rights ('IPRED') such as copyright and related rights, trademarks, designs or patents that was adopted in April 2004,[473] and evaluated in 2017.[474]

In **May 2016**, the **UK**'s Intellectual Property Office published its Policy Paper Protecting creativity, supporting innovation: IP enforcement 2020.[475]

In **2010**, the **International Law Association** established a Committee on Intellectual Property and Private International Law. The work of the Committee is ongoing.

Numerous institutions, such as the Centre for International Intellectual Property Studies (CEIPI) at the **University of Strasbourg**, provide detailed commentary on upcoming reform in this area.[476]

The well-known **ICANN** Uniform Domain-Name Dispute Resolution Policy (UDRP) adopted by ICANN-accredited registrars in all gTLDs, is a longstanding tool to resolve intellectual property disputes in the domain name sphere (such as cybersquatting).[477]

---

467. AZB & Partners. (2019, January 19). *Changing landscape of intermediary liability*. Retrieved from https://www.azbpartners.com/bank/changing-landscape-of-intermediary-liability/.

468. Torrent Freak. (2019, March 15). *Russia plans to block pirate sites without trial & de-anonymize their operators*. Retrieved from https://torrentfreak.com/russia-plans-to-block-pirate-sites-without-trial-de-anonymize-operators-190315/.

469. Ubertazzi, B. (2012). *Exclusive jurisdiction in intellectual property*. Tubingen: Mohr Siebeck, 139 (footnotes omitted).

470. Ubertazzi, B. (2012). *Exclusive jurisdiction in intellectual property*. Tubingen: Mohr Siebeck, 139 (footnotes omitted).

471. Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market COM/2016/0593 final - 2016/0280 (COD). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0593&from=EN.

472. Kayali, L. (2019, March 26). European Parliament approves overhaul of online copyright rules. *Politico*. Retrieved from https://www.politico.eu/article/european-parliament-approves-copyright-reform-in-final-vote/?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication.

473. European Union. *Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights*. OJL 157, 30.4.2004. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048R%2801%29.

474. European Commission. (2017, November 29). *Evaluation: Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights*. COM(2017) 431. Retrieved from https://ec.europa.eu/docsroom/documents/26601/attachments/2/translations/en/renditions/native.

475. United Kingdom Intellectual Property Office. *Protecting creativity, supporting innovation: IP enforcement 2020*. Retrieved from https://www.gov.uk/government/publications/protecting-creativity-supporting-innovation-ip-enforcement-2020.

476. Center for International Intellectual Property Studies. Retrieved from http://www.ceipi.edu/en.

477. ICANN. *Domain name dispute resolution policies*. Retrieved from https://www.icann.org/resources/pages/dndr-2012-02-25-en.

3.3.1.1 Aggressive cross-border acquisition of intellectual property

With intellectual property being one of the key safeguards for protecting innovation, it is unsurprising that fierce competition would arise around it. There is a clear cross-border dimension in this context, as different states compete to obtain innovation-driven advantages as the world heads toward an era of Industry 4.0. To put it simply, claims of jurisdiction facilitate control over intellectual property, which in turn, enables control over innovation potentially leading to economic, societal and military advantages.

> "To put it simply, claims of jurisdiction facilitate control over intellectual property, which in turn, enables control over innovation potentially leading to economic, societal and military advantages."

Much of the current debate in this field has centered on the relationship between the US and China. In 2015, then-US President Obama met with Chinese President Xi Jinping and reached agreement on a range of matters. Among other things, the two countries agreed "that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[478]

Yet, the US remains concerned that China unfairly facilitates the systematic acquisition of US companies by Chinese companies in order to obtain cutting-edge intellectual property rights. Furthermore, the US asserts that China conducts and supports hacking aimed at gaining access to sensitive commercial information and trade secrets of US companies.[479] The US has also pointed to how "China uses foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, and various administrative review and licensing processes, to require or pressure technology transfer from US companies."[480] Similar concerns about China's approach have been raised, for example, in Australia, New Zealand, Japan, Canada and the EU.[481]

Concerns about China's aggressive acquisition of intellectual property are part of a bigger picture – one where multiple states are fighting for advantages through technological superiority. The seriousness of this situation should not be underestimated, as the risk of escalation is obvious. As the largest states pursue technological superiority, there is an obvious risk that smaller states and developing states, in particular, will be used as pawns in this high-stakes game. There is also the risk of smaller and developing states having their autonomy limited and may prevent those states from freely formulating their own internet strategies.

3.3.1.2 Copyright used to restrict speech with cross-border effect

On September 18, 2018, the Japanese Cabinet Office presented a draft report advocating for legislation that would allow websites to be blocked for offering access to copyright-infringing content. The proposition, which came after the government asked ISPs to voluntarily block websites upon notice in April 2018, is controversial, and has been described as contrary to constitutional safeguards for freedom of speech.[482] Japan's controversial plans to amend copyright laws to criminalize the unlicensed downloading of all copyrighted content were abandoned in March 2019.[483]

This is merely one example of the potential for clashes between copyright

---

478. The White House: Office of the Press Secretary. (2015, September 25). *Fact Sheet: President Xi Jinping's state visit to the United States.* [Press Release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

479. See e.g.: United States of America v Zhang et al 13CR3132-H, Indictment. Retrieved from https://www.justice.gov/opa/press-release/file/1106491/download.

480. Office of the United States Trade Representative. (2018, March 22). *Findings of the investigation into China's acts, policies and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974.* Retrieved from https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF, at 19.

481. See e.g.: Cerulus, L. (2018, December 20). West accuses Beijing of 'extensive' cyber espionage. *Politico.* Retrieved from https://www.politico.eu/article/china-cyber-espionage-uk-us-accuses-beijing/, Fitzpatrick, M. (2013, April 15). Did China steal Japan's high-speed train. *Fortune.* Retrieved from http://fortune.com/2013/04/15/did-china-steal-japans-high-speed-train/, and Laskai, L. (2018, March 28). Why does everyone hate Made in China 2025? *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025.

482. Internet & Jurisdiction Policy Network. (2018, September). Japanese government presents draft report to implement website blocking to fight against copyright infringement. *I&J Retrospect Database.* Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7470_2018-09.

483. Torrent Freak. (2019, March 13). *Japan Abandons Tough Anti-Downloading Copyright Law.* Retrieved from https://torrentfreak.com/japan-abandons-tough-anti-downloading-copyright-law-190313/.

enforcement and the freedom of expression. As one interviewed expert noted, there are numerous examples of copyright laws being used as a tool to restrict content otherwise protected by freedom of expression.

The factually complex US *Garcia case* is an explicit example of this. In this case, an actress cast in a minor role in a film sought to prevent the publication, on YouTube, of another film that incorporated her scenes. Having failed to secure the content removal on other grounds, the actress sought, and was initially granted, a global takedown based on her alleged intellectual property rights in her performance.[484] The courts addressing the matter never considered the transnational dimension of the case, though, the decision was later overturned on copyright-related grounds.

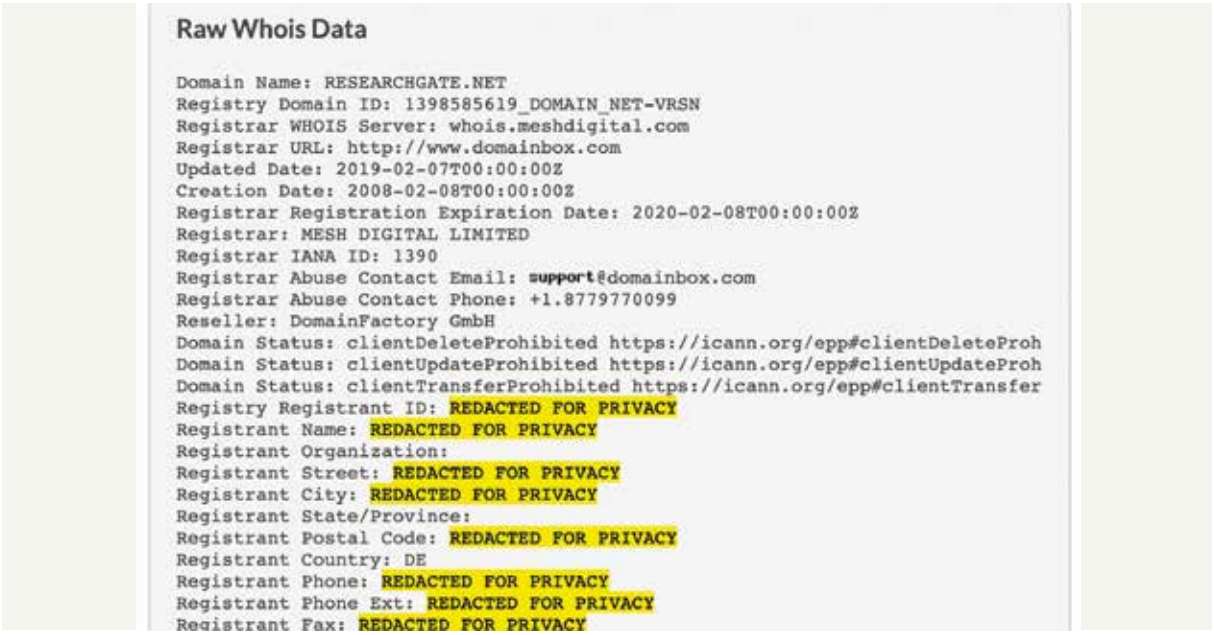
Another example with potential freedom of expression implications is a proposal from FairPlay Canada to establish a not-for-profit organization that would identify websites that engage in copyright piracy and require ISPs to block access to those websites. The Canadian Radio-Television and Telecommunications Commission rejected the proposal in October 2018.[485] As some interviewed experts stressed, copyright law is not uniform globally. Thus, where copyright law is used as the basis to remove content globally, content that is legal in some countries may be removed under laws where it is not lawful.

Some interviewed experts described controversial revisions to the EU Copyright Directive as granting expanded power to copyright holders, which could be abused to limit freedom of expression. The impacts of filtering measures in Article 13 of the 2018 draft EU Copyright Directive may be noted in this context. Another example is found in Tanzania's Electronic and Postal Communications (Online Content) Regulation 2018, which regulates content posted online with offenses for failing to remove content and imposes fees for bloggers and online media. Some interviewed experts also said copyright law could be used to suppress technology development and freedom of association.

3.3.1.3 Evolution of WHOIS, and its use by law enforcement and copyright associations

The WHOIS system – overseen by the internet Corporation for Assigned Names and Numbers (ICANN) – allows users to identify the registered owner of any given domain. As such, it has served as a valuable tool for a wide range of actors, including law enforcement and copyright associations – and, unfortunately, scammers and spammers.

But the information available on the WHOIS system has recently changed due to requirements outlined in the EU's GDPR, with registrars redacting personal information through their automated system.



Raw Whois Data

```
Domain Name: RESEARCHGATE.NET
Registry Domain ID: 1398585619_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.meshdigital.com
Registrar URL: http://www.domainbox.com
Updated Date: 2019-02-07T00:00:00Z
Creation Date: 2008-02-08T00:00:00Z
Registrar Registration Expiration Date: 2020-02-08T00:00:00Z
Registrar: MESH DIGITAL LIMITED
Registrar IANA ID: 1390
Registrar Abuse Contact Email: support@domainbox.com
Registrar Abuse Contact Phone: +1.8779770099
Reseller: DomainFactory GmbH
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProh
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProh
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransfer
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: DE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
```

Figure 1. WHOIS lookup of the domain researchgate.net as of January 2019.

484. Garcia v Google Inc 786 F.3d 733. Retrieved from http://cdn.ca9.uscourts.gov/datastore/general/2014/02/28/12-57302_opinion.pdf.

485. Canadian Radio-television and Telecommunications Commission. (2018, October 2). *CRTC denies FairPlay Canada's application on piracy websites on jurisdictional grounds.* [Press Release]. Canada.

This will impact the enforcement of intellectual property rights, including in instances where a rights holder seeks to take action against websites offering infringing content or goods. Yet, it has also been suggested that the WHOIS system is of limited use in pursuing copyright infringements. This is partly due to the fact that much of the information in the system is inaccurate, but also because the IP WHOIS tool, which shows who owns or controls a specific IP address, is generally more useful for this task.

This situation highlights the interpenetration of the three fields of focus in this Report: expression, economy and security. Here, a decision on data privacy (expression) in one region has quite unintended consequences on both economy and security on a global scale. This is a useful reminder of the need for coordination, cooperation and careful legal drafting.

3.3.2

E-commerce, competition law, marketing restrictions and consumer protection

Electronic commerce (e-commerce) comes in different forms, with a classic distinction between business-to-business (B2B) transactions, business-to-consumer (B2C) transactions and consumer-to-consumer (C2C) transactions. There is an emerging trend of regulators and legislators adopting tougher attitudes toward internet platforms when it comes to consumer protection. There are also early indications that internet companies' choice of forum and law clauses to impose on their users are not being enforced. Together, these two trends may have a significant impact in years to come.

An underlying and recurring theme in cross-border e-commerce is the need to balance predictability and flexibility. Predictability – for example, in the form of applicable laws and the geographic scope of jurisdiction – is necessary for business to confidently engage in e-commerce. This is particularly true given that e-commerce is characterized by both global markets and local laws.

> "There are early indications that internet companies' choice of forum and law clauses to impose on their users is not being enforced."

At the same time, parties that typically enter into transactions from a relatively weaker position, such as consumers, may require a high degree of flexibility so that the law accounts for their interests, over the predictable choices of court and law clauses by businesses. In some legal systems, consumers can rely upon the law and jurisdiction of their home country in their cross-border dealings with business, provided that certain criteria are met.[486] This degree of consumer protection is still rare, however, even though consumer protection laws are relatively common. A study by the UN Conference on Trade and Development (UNCTAD) illustrated that 97 of the 125 countries for which data could be accessed had adopted consumer protection legislation that related to e-commerce.[487] Of these, 61 were classed as developing or transition economies. However, the same study showed that it was not possible to obtain data for an additional 67 countries, which was interpreted to mean that online consumer protection in those countries is not being fully addressed. The incidence of consumer protection laws was shown to be particularly low in Africa.

The International Consumer Protection and Enforcement Network published an open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers.[488]

---

486. See e.g.: Regulation (EU) No 1215/ 2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I bis), Article 18, as exemplified in Joined cases C- 585/ 08 Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and C- 144/ 09 Hotel Alpenhof GesmbH v. Oliver Heller.

487. United Nations Conference on Trade and Development. *Online consumer protection legislation worldwide.* Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx.

488. International Consumer Protection and Enforcement Network. (2018, June 29). *Joint open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers.* Retrieved from https://www.icpen.org/news/902.

3.3.2.1 Tougher attitude towards internet platforms in e-commerce and competition law

With most internet platforms being based in the US, any action against these platforms in other parts of the world gives rise to potentially complex jurisdictional considerations. Importantly, the major internet platforms have adopted different corporate structures, which means that the jurisdictional grounds that may be relied upon in one scenario may not be sufficient to establish jurisdiction in another scenario. Available jurisdictional anchor points also vary depending on the area of substantive law in question.
For a long time, discussions on the regulation of digital platforms were predominantly concerned with ensuring that such actors were provided with sufficient protection to achieve their potential and blossom. Today, there are clear signs that the attitude towards internet platforms is hardening, both in industrialized and developing countries. In the context of marketing restrictions and consumer protection, for example, such an attitude is clearly visible in the Australian Competition and Consumer Commission (ACCC) inquiry into digital platforms.[489]
A further example is the 2018 EU Copyright Directive, which imposes greater responsibilities on certain digital platforms to stop users from posting copyright content. Additionally, the UN Internet Governance Forum's Dynamic Coalition on Platform Responsibility is working to produce model contractual provisions for internet platforms, with the ultimate aim of protecting users' human rights and enhancing platform responsibility.[490]
Another example of this hardening attitude was highlighted on August 1, 2017, when the Tanzanian Deputy Minister for Transport and Communications stated that the country should "guard against the misuse" of platforms like Facebook, Twitter and Instagram, "to make sure that while a person is free to say anything, there are mechanisms to hold them accountable for what they say."[491] In his statement, the Minister contrasted the American idea of unlimited freedom of speech online to the way China has regulated the internet, which includes blocking American social media platforms and "replacing them with their homegrown sites that are safe, constructive and popular."[492]
Another government initiative is the release by the French government of an interim mission report in May 2019 on the creation of a French framework to make social media platforms more accountable.[493]
One additional example can be seen in the December 2018 lawsuit filed by the US Attorney General against Facebook for a failure to protect its customers' personal data, and for allowing the political data firm Cambridge Analytica to access users' personal data.[494] In July 2019, the Federal Trade Commission imposed a US$5 billion penalty on Facebook for violating consumers' privacy.[495] Regulatory action against Facebook for the Cambridge Analytica data breach was taken by other countries, including Italy[496] and Canada.[497]
A tougher attitude towards internet intermediaries can also be seen in the field of competition law. For example, on July 18, 2018, the European Commission announced that it had fined Google €4.3 billion for breaking the EU's antitrust laws, arguing that the company had abused its Android market dominance.[498] Further, in March 2019, the European Commission fined Google €1.49 billion for abusive practices in online advertising.[499] The fact that further development may be expected in the EU is clear. For example,

---

489. Morrison, S. (2017, December 4). Letter to ACCC Chairman Rod Sims requiring ACCC inquiry into digital platforms. Retrieved from https://www.accc.gov.au/system/files/Ministerial%20direction.pdf. Final Report can be retrieved from Australian Competition and Consumer Commission. (2019, July 26) *Digital platforms inquiry - final report*. Retrieved from https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.
490. Internet Governance Forum. *Dynamic Coalition on Platform Responsibility*. Retrieved from https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-platform-responsibility-dcpr.
491. Internet & Jurisdiction Policy Network. (2017, August). Tanzania Deputy Minister of Communications calls for social media regulation similar to China's. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6235_2017-08.
492. Internet & Jurisdiction Policy Network. (2017, August). Tanzania Deputy Minister of Communications calls for social media regulation similar to China's. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6235_2017-08.
493. Creating a French Framework to make social media platforms more accountable. (2019, May). Retrieved from https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Régulation%20des%20réseaux%20sociaux%20-ENG.pdf.
494. District of Columbia v Facebook Inc, Complaint. Retrieved from http://oag.dc.gov/sites/default/files/2018-12/Facebook-Complaint.pdf.
495. Internet & Jurisdiction Policy Network. (2019, July). Federal Trade Commission fines Facebook US$5 billion and orders oversight layers for data protection. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiY2FtYnJpZGdlIGFuYWx5dGljYSIsImZyb20iOiIyMDE5LTAxIiwidG8iOiIyMDE5LTA4In0=.
496. Internet & Jurisdiction Policy Network. (2019, June). Italy fines Facebook for data breach. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaXRhbHkiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9.
497. Internet & Jurisdiction Policy Network. (2019, April). Canada Privacy Commissioner's investigation concludes that Facebook broke Canadian privacy laws. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiY2FuYWRhIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==.
498. European Commission. (2018, July 18). *Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine*. [Press Release] Retrieved from http://europa.eu/rapid/press-release_IP-18-4581_en.htm.
499. European Commission. (2019, March 20). *Statement by Commissioner Vestager on Commission decision to fine Google € 1.49 billion for abusive practices in online advertising*. [Press Release]. Brussels. Retrieved from https://europa.eu/rapid/press-release_STATEMENT-19-1774_en.htm.

in September 2019, it was reported that the European Competition Commissioner, Margrethe Vestager, saw reasons to "introduce rules to specifically cover tech companies and their use of data".[500]

In February 2019, Germany's antitrust office ruled that Facebook is abusing its virtual monopoly in social media by combining data from Instagram, WhatsApp and third party websites.[501] A further example of a stricter approach in this context is the December 2018 announcement that "India will ban e-commerce companies [...] from selling products from companies in which they have an equity interest."[502] India published a Draft National e-Commerce Policy in February 2019, calling for increased protection of consumer rights and data localization.[503]

In the US, anti-trust initiatives targeting the tech industry are being pursued both on a federal level,[504] and on a state level.[505] As at July 2019, the UK Competition and Markets Authority is reportedly investigating Facebook and Google's advertising market domination in the UK.[506]

There are also moves to establish specific regulatory bodies. For example, the Japanese government reportedly plans to set up a regulatory body to examine the competitive practices of the major social media platforms and make anti-trust recommendations.[507] The UK House of Lords has released a 'Regulating in a Digital World' report recommending the creation of a Digital Authority to coordinate existing regulators.[508] Additionally, the US Federal Trade Commission announced in 2019 the launch of a Task Force to Monitor Technology Markets.[509]

In December 2017, the OECD held a roundtable on the extraterritorial reach of competition remedies more broadly.[510]

3.3.2.2 Specifically regulated industries

Certain products, and indeed certain industries, are subject to specific regulation, restrictions or bans. The sale of weapons, alcohol, narcotics, pharmaceuticals and hazardous chemicals are all examples of this. The provision of gambling services is another area associated with specific regulation.[511] This gives rise to particular issues in the online environment, given the ease with which products are bought and sold across borders. Particularly, the regulation of online pharmacies has gained a considerable degree of attention over the past years. The Brussel Principles on the Sale of Medicines Over the Internet[512] bring attention to the numerous conflicting policy considerations at stake, for example:

1. The World Health Organization (WHO) estimates that over two billion people lack regular access to essential medical products;
2. Major public health concerns arise where quality control cannot be assured;
3. The marked actors include both legitimate online pharmacies and rogue operators; and
4. Cross-border competition may benefit availability and lower prices.

In such a landscape, international coordination and cooperation is a necessity.

---

500. Yun Chee, F. (2019, September 13). EU may need to regulate tech giants' data use: EU antitrust chief. *Reuters*. Retrieved from https://www.reuters.com/article/us-eu-antitrust-data-idUSKCN1VY1GU.

501. Kottasova, I. (2019, February 7). Germany orders Facebook to change the way it gathers data. *CNN Business*. Retrieved from https://edition.cnn.com/2019/02/07/tech/facebook-germany-data-collection/index.html.

502. Ahmed, A. & Phartiyal, S. (2018, December 27). India tightens e-commerce rules, likely to hit Amazon, Flipkart. *Reuters*. Retrieved from https://www.reuters.com/article/us-india-ecommerce/india-tightens-e-commerce-rules-likely-to-hit-amazon-flipkart-idUSKCN1OP14M.

503. Internet & Jurisdiction Policy Network. (2019, February). India: Proposed E-Commerce Policy calls for increased data localization and increased protection of data privacy and consumer rights. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kaWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9.

504. Gupta, N,. (2019, July 24). Why DOJ Antitrust Review Is bad news for Facebook. *Market Realist*. Retrieved from https://articles2.marketrealist.com/2019/07/doj-antitrust-review-is-bad-news/.

505. New York Attorney General. (2019, September 6). *AG James investigating Facebook for possible antitrust violations*. [Press Release]. New York. Retrieved from https://ag.ny.gov/press-release/2019/ag-james-investigating-facebook-possible-antitrust-violations .

506. Sweeney, M. (2019, July 4). Google and Facebook under scrutiny over UK ad market dominance. *The Guardian*. Retrieved from https://www.theguardian.com/business/2019/jul/03/google-facebook-investigated-over-dominance-of-uk-digital-advertising-market.

507. White, S. (2019, February). Japan sets sights on tighter anti-trust regulations for Big Tech. *Reuters*. Retrieved from https://www.reuters.com/article/us-japan-economy-tech/japan-sets-sights-on-tighter-anti-trust-regulations-for-big-tech-idUSKCN1Q20YB?feedType=RSS&feedName=technologyNews.

508. UK House of Lords Select Committee on Communications. (2019, March). *Regulating in a digital world*. Retrieved from https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf.

509. Federal Trade Commission. (2019, February 26). *FTC's Bureau of Competition launches task force to monitor technology markets*. [Press Release]. Retrieved from https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

510. OECD. (2017, December, 5). *Extraterritorial reach of competition remedies*. Retrieved from http://www.oecd.org/daf/competition/extraterritorial-reach-of-competition-remedies.htm.

511. See e.g.: Trimble, M. (2013). Proposal for an international convention on online gambling. In Cabot, A. & Pindell N. (Eds.), *Regulating internet gaming*. Retrieved from https://ssrn.com/abstract=2089935 and Hörnle, J. & Zammit, B. (2010). *Cross-border online gambling law and policy*. Cheltenham, United Kingdom: Edward Elgar.

512. Brussel principles on the sale of medicines over the Internet. Retrieved from https://www.brusselsprinciples.org/.

3.3.2.3 Non-enforcement of choice of forum and choice of law clauses

Studies have repeatedly highlighted that consumers very rarely read the terms and conditions to which they arguably 'agree' – e.g., by clicking 'I agree' (so-called click-wrap agreements) or by merely using a website (so-called browse-wrap agreements). Some have cited this in questioning the validity of choice of forum clauses (determining where the parties can sue) and choice of law clauses (determining which country's law will govern disputes between the parties) included in such agreements. This issue also arises in relation to clauses nominating arbitration as a mandatory dispute resolution process, especially in consumer contracts.[513]

In the Supreme Court of Canada's June 2017 decision in *Douez v. Facebook, Inc.*,[514] the majority (4-3) of the Court held Facebook's forum selection clause (which nominated a California court) unenforceable. The matter arose out of a data privacy case brought by a British Columbia resident against Facebook. Facebook had argued that disputes concerning its terms of use must be resolved in California, but the Supreme Court ruled otherwise, arguing that it would be more convenient to have Facebook's books and records made available for inspection in British Columbia, rather than requiring the defendant to travel to California to advance her claim.[515]

In 2016, the CJEU was invited to consider whether Amazon EU's choice of law clause was unfair under EU consumer law.[516] Advocate General Saugmandsgaard Øe concluded that Amazon EU's choice of law clause cannot override the option of litigating under the consumer's home state law, as created by the Rome I Regulation. The clause cannot, therefore, be seen to unfairly exclude the consumer from exercising this option. However, the clause Amazon EU used may mislead consumers into believing that they do not have the right under the Rome I Regulation, and this potential to mislead makes the term unfair under relevant EU consumer law. This reasoning was also adopted by the Court.[517] It is noteworthy that the same reasoning can be applied to any clause in a consumer contract where that term does not adequately reflect the provisions of mandatory law.

It remains to be seen whether these developments are indicative of a trend against upholding choice of forum and choice of law clauses in online agreements, or whether adherence to so-called 'party-autonomy' – which ultimately presents users with unilaterally predetermined contractual terms on a take-it-or-leave-it basis – will be reaffirmed. As far as the EU is concerned, some clarity was gained from a case concerning the status of agreements by way of a pre-checked checkbox, which users must 'unselect' to refuse their consent.[518] Advocate General Szpunar of the CJEU opined in March 2019, that such pre-checked boxes do not count as valid consent.[519] On 1 October 2019, the CJEU ruled, that: "the consent referred to in those provisions [Article 2(f) and of Article 5(3) of 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] is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent."[520]

The French data protection authority (CNIL) has also issued new Guidelines on Cookies and Tracking Devices to be consistent with the requirement for valid consent in the GDPR.[521]

As noted by one surveyed expert, the complexity is augmented by the fact that there is no universal definition of who is a 'consumer'.

---

513. Garnett, R. (2017). Arbitration of cross-border consumer transactions in Australia: A way forward?. *Sydney Law Review*, 39(4), 569-599.

514. 2017 SCC 33. See further: Harris, L. W. (2019). Understanding public policy limits to the enforceability of forum selection clauses after Douez v Facebook. *Journal of Private International Law*, 15(1), 50-96.

515. Internet & Jurisdiction Policy Network. (2017, June). Canadian Supreme Court says Facebook privacy lawsuit can be heard in British Columbia instead of California. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6109_2017-06.

516. Namely: Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

517. Case C-191/15 Verein für Konsumenteninformation v Amazon EU Sàrl.

518. Case C-673/17 Planet49.

519. Opinion of Advocate General Szpunar in Planet49 (Case C-673/17).

520. Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3969308, para #.

521. Hunton, A. K. (2019, June 23). *CNIL publishes new guidelines on cookies and similar technologies*. Retrieved from https://www.huntonprivacyblog.com/2019/07/23/cnil-publishes-new-guidelines-on-cookies-and-similar-technologies/.

3.3.3

Taxation – the intersection of jurisdictional complexities and national economy

Several surveyed and interviewed experts pointed to taxation as a particularly significant area of development for the coming years, and an area deserving detailed attention from a cross-border perspective. Jurisdictional complications arise, for example, due to the presence of multiple anchor points that can potentially be used for taxation purposes; taxation may be founded upon the location of users, (branch) offices, headquarters, servers, etc. Increasing attention is being directed toward the taxation of major internet platforms, in particular. Steps are also taken to ensure the effective collection of taxes online.[522]

Taxation is also an area in which we see an emerging trend of increased international cooperation. For example, in July 2018 the Joint Chiefs of Global Tax Enforcement (known as the J5) was announced.[523] Comprised of authorities from Australia, Canada, The Netherlands, UK and US, the J5 aims to combat transnational tax crime through increased enforcement collaboration. Among other areas, their work will focus on cyber-enabled identity crime as a way to evade tax, and on cryptocurrencies on the Darknet. This brings attention to the connection between work on taxation on the one hand, and the investigation and prosecution of cybercrime – including asset confiscation – on the other hand.[524] Jurisdictional issues are key concerns in this context.

The underlying issue is that as more transactions take place online, taxing traditional commerce will not generate as much revenue as it once did. If a government is to maintain its revenue levels, it must either increase the tax on offline transactions or tax online commercial activities. Much is at stake, and the debate about e-commerce taxation has sparked discussions aimed at a comprehensive reform of the international tax system.

Some have argued against these points, maintaining that taxation slows down the internet's development in general, and e-commerce in particular. Bearing in mind the complex nature of the international tax system, there is an obvious risk that inexperienced traders will not comply with the law due to ignorance. While ignorance of the law is not a defense, as such, some form of reasonableness assessment may be appropriate. It has also been suggested that the slow pace of taxation development cannot keep up with the rapid development of technology, which risks leading to undesirable results.

---

522. See e.g.: El Director General De Impuestos y Aduanas Nacionales. (2018, October 19). Resolución Número 000051. Retrieved from https://www.dian.gov.co/normatividad/Normatividad/Resoluci%C3%B3n%20000051%20de%2019-10-2018.pdf.

523. Joint Chiefs of Global Tax Enforcement. (2018, July 2). *Tax enforcement authorities unite to combat international tax crime and money laundering.* [Press Release]. Montreal. Retrieved from https://www.irs.gov/pub/irs-utl/j5-media-release-7-2-18.pdf.

524. See e.g.: Australian Taxation Office. *Organised crime*. Retrieved from https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Organised-crime/.

3.3.3.1 Taxing data and the search for a new basis for taxation

As the OECD has noted, the international tax structures in operation today were designed more than a century ago.[525] Modernization, including the search for a new basis for taxation is, therefore, a natural development aimed at addressing base erosion and profit shifting (BEPS). In February 2019, the OECD released a Public Consultation Document: Addressing the Tax Challenges of the Digitalisation of the Economy.[526]

The idea of taxing data is not new and considering the difficulties in applying traditional tax schemes to e-commerce and other online activities, a range of new tax schemes have been suggested. Common among all of these schemes is that they seek to tax the technology behind the transactions. More recent suggestions include taxation based on turnover, taxation based on offering services, taxation based on location, and taxation based on targeting, incorporation, or users served.

One of the most debated recent proposals is the European Commission's now-stalled proposal for a digital services tax (DST).[527] The failure of this initiative to gain sufficiently broad support has driven individual EU Member States, such as France, to pursue their own tax reform initiatives.[528] The French digital tax initiative has been criticized by US technology companies who warn of increased prices and harm to the digital economy.[529] Australia's Multinational Anti-Avoidance Law (MAAL), which came into effect on December 11, 2015, is another example of a recent tax reform initiative aimed at the technology sector.[530]

Examples of developments in this field can be found from around the world. For example, on 9 September 2019, it was reported that Mexico is considering extending a sales tax to foreign online businesses.[531] Uganda, in a unique approach, has opted to pilot a scheme taxing its citizens' use of social media platforms like Facebook, Skype, Twitter, and WhatsApp.[532] In Cameroon, the Finance Act 2019 contains a tax on software and application downloads produced outside the country.[533]

Furthermore, numerous states in Asia – including Indonesia,[534] Singapore,[535] Thailand,[536] Vietnam,[537] and Malaysia[538] – are working on implementing e-commerce tax initiatives.

It was reported in June 2019, that the G20 Finance Ministers agreed to develop rules to crack down on loopholes employed by global tech companies to reduce taxes.[539]

---

525. OECD. (2018). *Tax challenges arising from digitalisation: Interim report 2018:* Retrieved from http://dx.doi.org/10.1787/9789264293083-en, at 3.

526. OECD. (2019). *Public consultation document: Addressing the tax challenges of the digitalisation of the economy.* Retrieved from http://www.oecd.org/tax/beps/public-consultation-document-addressing-the-tax-challenges-of-the-digitalisation-of-the-economy.pdf. For the work of the OECD on this topic, see also: OECD. (2019). *Programme of work to develop a consensus solution to the tax challenges arising from the digitalisation of the economy.* Retrieved from www.oecd.org/tax/beps/programme-of-work-to-develop-aconsensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.htm.

527. Smith-Meyer, B. (2018, November 28). EU digital tax 'dead' as countries eye national paths. *Politico Pro.* Retrieved from https://www.politico.eu/pro/eu-digital-tax-dead-as-countries-eye-national-paths/. See further: Council of the European Union. *Digital Taxation.* Retrieved from https://www.consilium.europa.eu/en/policies/digital-taxation/.

528. Kayali, L. (2018, December 17). French tax on Google, Facebook to apply from January 1, 2019. *Politico.* Retrieved from https://www.politico.eu/article/french-tax-on-google-facebook-to-apply-from-january-1-2019/.

529. Ekblom, J. & Shepardson, D. (2019, August 20). U.S. tech industry leaders: French digital service tax harms global tax reform. *Reuters.* Retrieved from https://www.reuters.com/article/us-france-tax-usa/u-s-tech-industry-leaders-french-digital-service-tax-harms-global-tax-reform-idUSKCN1V91UC.

530. Australian Taxation Office. (2017, August 10). *Combating multinational tax avoidance – a targeted anti-avoidance law.* Retrieved from https://www.ato.gov.au/Business/International-tax-for-business/In-detail/Doing-business-in-Australia/Combating-multinational-tax-avoidance---a-targeted-anti-avoidance-law/.

531. Eschenbacher, S., Graham, D., Love, J., & Solomon, D. B. (2019, September 9). Mexico eyes sales tax on digital businesses to boost revenue. *Reuters.* Retrieved from https://www.reuters.com/article/us-mexico-budget-digitalplatforms/mexico-eyes-sales-tax-on-digital-businesses-to-boost-revenue-idUSKCN1VU1H1.

532. Internet Society. (2018, September). *The internet and extra-territorial application of laws.* Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf, p. 9.

533. Toussi, S. (2019, September 12). Overview of Cameroon's digital landscape. *Collaboration on International ICT Policy in East and Southern Africa.* Retrieved from https://cipesa.org/2019/09/overview-of-cameroons-digital-landscape/.

534. Jefriando, M. (2019, March 29). Indonesia retracts e-commerce regulation to avoid confusion. *Reuters.* Retrieved from https://www.reuters.com/article/us-indonesia-tax-ecommerce/indonesia-retracts-e-commerce-regulation-to-avoid-confusion-idUSKCN1RA0ZU.

535. Inland Revenue Authority of Singapore. *E-Commerce.* Retrieved from https://www.iras.gov.sg/irashome/GST/GST-registered-businesses/Specificbusiness-sectors/e-Commerce/.

536. TechInAsia. (2019, August 27). *In brief: Thailand to implement ecommerce tax in 2020.* Retrieved from https://www.techinasia.com/thailand-implement-ecommerce-tax-2020.

537. Samuel, P. (2019, July 25). Vietnam's tax administration law reform to take effect in July 2020. *Vietnam Briefing.* Retrieved from https://www.vietnam-briefing.com/news/vietnams-tax-administration-law-reform-take-effect-july-2020.html/.

538. EY. (2019). *Malaysia publishes updated Guidelines on Taxation of e-Commerce Transactions.* Retrieved from https://www.ey.com/gl/en/services/tax/international-tax/alert--malaysia-publishes-updated-guidelines-on-taxation-of-e-commerce-transactions.

539. White, S. & Strupczewski, J. (2019, June 8). G20 agrees to push ahead with digital tax: communique. *Reuters.* Retrieved from https://www.reuters.com/article/us-g20-japan-tax/g20-agrees-to-push-ahead-with-rules-on-corporate-tax-targeting-tech-giants-idUSKCN1T903D?feedType=RSS&feedName=technologyNews.

3.3.3.2 Taxation and data localization

There are at least two points of connection between taxation and data localization. First, taxation may be a driving force for data localization (see further: Chapter 4.2.7) in cases where taxation is based on data location; that is, companies may choose to locate their data centers at specific locations in the pursuit of tax advantages.

Second, taxation may be a driving force for data localization in cases where countries' tax laws require that certain tax and accounting records be held at the business's premises. Some of these laws are recent. In April 2018, for example, the Reserve Bank of India released a directive mandating all entities to store payments systems data related to user transactions only within India's national boundaries.[540] The pronounced aim was to ensure better monitoring and unfettered supervisory access to data stored with payment system providers. Such laws, however, pre-date widespread use of cloud computing, and may in fact pre-date widespread internet usage. Nevertheless, it remains a fact that restrictions on access to payment systems and payment data can be used as tools of foreign policy.

3.3.4

Internet of Things (IoT) – everything transferring data everywhere

The concept of the Internet of Things (IoT) refers to situations where internet connectivity is extended beyond traditionally networked devices (such as computers and smartphones) to physical, previously unconnected objects (such as fridges, light bulbs and cars). While many aspects of the IoT remain to be crystalized, there is no doubt that the IoT revolution will cause a massive increase in cross-border flows of both personal and non-personal data, including machine-to-machine (M2M) data flows.

Interviewed experts made a range of interesting observations in relation to the IoT. For example, one interviewed expert pointed to the law enforcement benefits of being able to track vehicles even where they cross-borders. Another noted that the IoT may make attribution easier in criminal investigations. However, the same interviewed expert also remarked that if the data generated by the IoT is stored in the cloud – which is commonly the case – it will lead to an even greater volume of law enforcement requests for data.

Some interviewed experts noted that the IoT is prompting data-driven internet companies to expand into markets that were previously non-digital. Car manufacturing and water supply systems are two examples of this trend. This merging of offline and online spheres expands the role of data – including cross-border data flows – and will, one interviewed expert remarked, give rise to cross-border legal problems.

The IoT has seen a rapid advancement, and many aspects of it are already in operation. For example, McKinsey estimates that 127 new devices are connecting to the internet every second.[541] Nevertheless, the IoT still faces several challenges, and the business community seems ill-prepared. A 2018 PwC study, Global State of Information Security Survey, showed that only 34% of their surveyed experts "say their organizations plan to assess internet of things (IoT) security risks across the business ecosystem."[542]

Some of the key challenges facing the IoT include:

- security and privacy concerns;
- a lack of technical standards;
- product safety concerns;
- concerns about inadequate bandwidth;
- environmental sustainability concerns;
- control, responsibility and liability concerns
- concerns about data ownership; and
- interoperability limitations.

Several of these concerns highlight the necessity of cross-border cooperation and coordination.

Furthermore, as IoT development relies on faster mobile networks, the speed with which 5G networks become available is of great importance and may in fact set the pace for IoT uptake. In this, we find a convergence of several of the major topical trends discussed in the Chapter 3. The US-China trade conflict, involving both digital protectionism (Chapter 3.3.6.1) and aggressive cross-border acquisition of intellectual property

---

540. Reserve Bank of India. (2018, April 6). *Storage of payment system data*. Retrieved from https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

541. Baroudy, K., Kishore, S., Nair, S. & Patel, M. (2018, March). Unlocking value from IoT connectivity: Six considerations for choosing a provider. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/industries/high-tech/our-insights/unlocking-value-from-iot-connectivity-six-considerations--for-choosing-a-provider.

542. PwC. (2018). *How businesses can build the resilience needed to withstand disruptive cyberattacks*. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html.

(Chapter 3.3.1.1), has in part, centered on the business practices of Chinese tech giant Huawei. This, together with cybersecurity concerns (Chapter 3.2.4) about Huawei products have led some countries to ban the company's products, and this is likely to delay the deployment of 5G, which is a necessary building block for widespread IoT adoption.

This complex matrix of cross-border interests and concerns highlights the interconnectedness of the issues discussed in this Chapter. It also brings attention to the tension between rapid technological deployment on the one hand, and careful consideration of cyber security implications on the other.

Some notable initiatives and developments in the IoT sphere include the following:
In **September 2019**, the **Internet Society** published a policy brief on privacy and the Internet of Things.[543]
Responding to the call of stakeholders engaged in the **Internet & Jurisdiction Policy Network**, a one-day workshop on the Internet of Things was organized in Berlin, Germany in **April 2019**. The meeting aimed to help frame and foster a common understanding of the cross-border legal challenges with regards to the Internet of Things, explore the need for and benefits of multistakeholder coordination and cooperation, and explore potential avenues for developing operational solutions and policy standards to handle the new cross-border legal challenges at the nexus of the Internet of Things, AI, and the Fourth Industrial Revolution.
The **US Federal Trade Commission** (FTC) issued an FTC staff report on privacy in IoT titled Internet of Things: Privacy and Security in a Connected World.[544]
In **February 2018**, **Siemens** started working with partners from industry, government and society to sign a 'Charter of Trust' aimed at three objectives: (1) Protecting the data of individuals and companies; (2) Preventing damage to people, companies and infrastructures; and (3) Establishing a reliable foundation on which confidence in a networked, digital world can take root and grow.[545]
In **2017**, the **World Bank Group** published a Report titled Internet of things: the new government to business platform - a review of opportunities, practices, and challenges.[546]
The **Internet Governance Forum (IGF) Dynamic Coalition on the Internet of Things** is seeking to achieve best practice in relation to the IoT particularly addressing safety, security and privacy.[547]
In **2017**, **Google Cloud** announced the global availability of its IoT Core service.[548]
In an example of cross-border internet cooperation in the IoT field, in **2016**, a group of major telecommunications providers formed the **IoT World Alliance**.[549]

543. Internet Society. (2019, September 19). *Policy brief: IoT privacy for policymakers.* Retrieved from https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/.

544. Federal Trade Commission. (2019, January). *Internet of Things: Privacy and Security in a Connected World.* Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

545. Siemens. (2018). *Charter of Trust on cybersecurity.* Retrieved from https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/180514-charter-of-trust-standard-presentation-v03.pdf.

546. World Bank Group. (2017). *Internet of Things: The new government to business platform - a review of opportunities, practices, and challenges.* Retrieved from http://documents.worldbank.org/curated/en/610081509689089303/internet-of-things-the-new-government-to-business-platform-a-review-of-opportunities-practices-and-challenges.

547. Internet Governance Forum. (2018). *IGF 2018 DC Internet of Things: Global good practice in IoT: a call for commitment.* Retrieved from https://www.intgovforum.org/multilingual/content/igf-2018-dc-internet-of-things-global-good-practice-in-iot-a-call-for-commitment.

548. Google Cloud. *Cloud IoT Core.* Retrieved from https://cloud.google.com/iot-core/?utm_source=bing&utm_medium=cpc&utm_campaign=japac-AU-all-en-dr-bkws-all-all-trial-e-dr-1003987&utm_content=text-ad-none-none-DEV_c-CRE_75110457775562-ADGP_Hybrid+%7C+Bing+SEM+%7C+BKWS+%7E+T3+%7C+EXA+%7C+Others+%7C+M%3A1+%7C+AU+%7C+en+%7C+IOT-KWID_43700033430033742-kwd-75110536580611:loc-9&utm_term=KW_iot&gclid=CMn78pnbu94CFQ7kjgodz00CXA.

549. IoT World Alliance. Retrieved from http://www.iotworldalliance.org/#section_intro.

3.3.4.1 Smart connected homes in smart connected cities

Much can be gained from the development of so-called smart cities, including smart power and water grids. Greater efficiencies, for example, can generate cost savings and deliver environmental benefits. Developments such as self-driving cars can cut costs, help save the environment and minimize accidents.

Smart homes equipped with smart thermostats, smart appliances and connected heating, lighting and electronic devices can be controlled remotely via computers, smartphones or other mobile devices. This might minimize costs, while offering both convenience and environmental advantages.

Connected wearable devices with sensors can collect, analyze and communicate user data to provide multiple user benefits, and may also be used to increase public safety.

> "As any increase in international contacts comes with a likely increase in international disputes, the move to smart homes and smart cities will likely create additional pressure on international dispute resolution mechanisms, and may even create new jurisdictional anchor points."

With the internet being a global network, this interconnectivity creates direct links between homes and cities in different countries, and with providers that may be based anywhere in the world. As any increase in international contacts comes with a likely increase in international disputes, the move to smart homes and smart cities will likely create additional pressure on international dispute resolution mechanisms and may even spark the creation of new jurisdictional anchor points.

Some interviewed experts noted that, as tech companies move into new industries such as car manufacturing, mobility systems and water supply management, they enter an environment characterized by a much greater level of regulation, and different safety and security considerations.

3.3.4.2 Wearable e-health

Wearable technology such as smart watches can accurately record a wide range of sensitive health data. The relevant user data is then typically stored in cloud computing solutions. As a result, cross-border data transfers are common, and jurisdictional issues may arise in case of leaks, such as those reported in relation to Fitbit in January 2016,[550] PumpUp in June 2018[551] and Garmin in October 2018.[552]

In the context of both smart cities and the more personal matters discussed here, careful attention must be given to respecting data privacy rights, ensuring cybersecurity, and not stifling innovation. Given that providers and users of smart devices are frequently not based in the same country, there is a clear need for international coordination and cooperation.

3.3.5

Blockchain – still a solution searching for a problem?

Since the publication of Satoshi Nakamoto's original white paper in 2008,[553] blockchain technology has captured the imagination of the world, and is extensively discussed in academic literature, policy documents and the media. To date, however, few jurisdictional issues have been highlighted, and the topic of blockchain technology attracted limited attention during interviews for this Report.

In basic terms, blockchain technology may be described as a global distributed spreadsheet or as a 'trusted public ledger' – or indeed, as preferred by some, a 'trustless public ledger'. The aim of removing the 'middleman' has been a central driving force behind blockchain technology. The main rationale for bitcoin, for example, as outlined in Nakamoto's original white paper, was the need for an electronic payment system that would allow any two willing parties to transact directly with one another without the need for a trusted third party. In the blockchain, cryptographic proof removes the need for trust.

---

550. McGee, M.K. (2016, January 11). Fitbit hack: What are the lessons? *Data Breach today*. Retrieved from https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793.

551. McGee, M.K. (2018, June 4). Another fitness app exposes users' data. *Data Breach today*. Retrieved from https://www.databreachtoday.com/another-fitness-app-exposes-users-data-a-11055.

552. Osborne,C. (2018, October 9). Garmin's Navionics exposed data belonging to thousands of customers. *ZD Net*. Retrieved from https://www.zdnet.com/article/garmins-navionics-exposed-data-belonging-to-thousands-of-boat-owners/.

553. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf.

Sparked by the strong uptake of Bitcoin, blockchain technology is sometimes described as analogous to bitcoin. But bitcoin is merely one of many cryptocurrencies, and cryptocurrencies are just one of the many uses of blockchain technology. So-called smart contracts (discussed below) are another example of a commonly discussed use of blockchain technology, and there are both public and private blockchains, as well.

Indeed, blockchain's potential is such that a team of developers in 2014 announced plans for a peer-to-peer network that would work without centralized servers.[554] Similar to the TOR network, or the mining principle behind bitcoin, individual computers would serve as nodes that would route network traffic in a decentralized and encrypted way without ISPs.[555] The infrastructure would be financed through micro-payments in relation to the traffic managed by individual nodes. A Scottish company claims to have already developed a similar network called MaidSafe.[556]

In 2018, the Dubai International Financial Centre (DIFC) Courts, together with Smart Dubai, began working to create the world's first blockchain-enabled court, including a blockchain-enabled scheme for the verification of monetary court judgments that can be enforced across borders.[557] In September 2018, China's Supreme People's Court (SPC) issued a judicial interpretation on the hearing of cases by internet courts. The judicial interpretation made clear that evidence authenticated and presented using blockchain technology is binding in legal disputes heard by the three internet courts in Hangzhou, Beijing, and Guangzhou. [558] Despite the rapid uptake and enormous interest, cryptocurrencies, and blockchain technology in general, face several technical and economic challenges. Scalability is often cited as one challenge, though, it may also be an advantage in that the greater the number of users, the greater the security of the blockchain.

Data privacy issues are frequently raised, as well.[559] For example, although solutions to this issue may evolve, there is a fundamental clash between the right to amend incorrect personal data commonly found in data privacy laws, and the 'immutable' nature of the blockchain. This immutable nature is exemplified by the fact that every bitcoin transaction that has ever been performed is stored publicly, by design, on the bitcoin peer-2-peer (P2P) network. And as far as cryptocurrencies are concerned, volatility remains a serious issue. For example, in September 2019, a wide range of popular cryptocurrencies dropped 15-22% in value.[560]

In addition, the computing power that the blockchain requires has serious environmental implications. A 2018 study published in the peer-reviewed journal *Nature Climate Change* estimated that, in 2017 alone, the use of bitcoins emitted 69 million metric tons of CO_2.[561] The researchers behind the study found that "if Bitcoin is incorporated, even at the slowest rate at which other technologies have been incorporated, its cumulative emissions will be enough to warm the planet above 2°C in just 22 years. If incorporated at the average rate of other technologies, it is closer to 16 years."[562] This is an interesting illustration of the intersection of the online and offline worlds, with the online activities in one state, or a group of states, having extraterritorial effects in the offline environment in other states.

3.3.5.1 Cryptocurrencies as enablers of cross-border trade and crime

Because a cryptocurrency such as Bitcoin does not recognize national borders, it is an obvious enabler of cross-border trade – both lawful and unlawful. Indeed, Bitcoin is often discussed in the context of the online sale of illegal products such as weapons and drugs, as well as other criminal activities. Europol's 2018 Internet Organ-

---

554. BBC News. (2014, January 23). *Bitcloud developers plan to decentralise internet*. Retrieved from http://www.bbc.co.uk/news/technology-25858629.

555. Internet & Jurisdiction Policy Network. (2014, January). Bitcoin developers plan to create a new, decentralized internet. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-4940_2014-01.

556. Powles, J. (2014, January 27). Scottish company Maidsafe claims to have built a bitcloud-like system. *Wired*. Retrieved from http://www.wired.co.uk/news/archive/2014-01/27/maidsafe-bitcloud.

557. Dubai International Financial Centre. (2018, July 30). *DIFC Courts and Smart Dubai launch joint taskforce for world's first Court of the Blockchain*. [Press Release]. Retrieved from https://www.difc.ae/newsroom/news/difc-courts-and-smart-dubai-launch-joint-taskforce-worlds-first-court-blockchain/.

558. Zhang, L. (2018, September 21). China: Supreme Court issues rules on internet courts, allowing for blockchain evidence. *Library of Congress*. Retrieved from http://www.loc.gov/law/foreign-news/article/china-supreme-court-issues-rules-on-internet-courts-allowing-for-blockchain-evidence/.

559. See further: Kuner. C., Cate, F., Lynskey, O., Millard, C., Loideain, N. W. & Svantesson, D. (2018, May). Blockchain versus data protection. *International Data Privacy Law*, 8(2), 103–104. Retrieved from https://academic.oup.com/idpl/article/8/2/103/5047578.

560. Bambrough, B. (2019, September 24). Bitcoin, Ethereum, Ripple's XRP, And Litecoin In shock meltdown. *Forbes*. Retrieved from https://www.forbes.com/sites/billybambrough/2019/09/24/bitcoin-ethereum-ripples-xrp-and-litecoin-in-shock-meltdown/#700f5fd73391.

561. University of Hawaii at Manoa. (2018, October 29). Bitcoin can push global warming above 2 degrees C in a couple decades. *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2018/10/181029130951.htm.

562. University of Hawaii at Manoa. (2018, October 29). Bitcoin can push global warming above 2 degrees C in a couple decades. *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2018/10/181029130951.htm.

ised Crime Threat Assessment, notes:

> "Previous reports indicated that criminals increasingly abuse cryptocurrencies to fund criminal activities. While Bitcoin has lost its majority of the overall cryptocurrency market share, it still remains the primary cryptocurrency encountered by law enforcement. In a trend mirroring attacks on banks and their customers, cryptocurrency users and facilitators have become victims of cybercrimes themselves. Currency exchangers, mining services and other wallet holders are facing hacking attempts as well as extortion of personal data and theft. Money launderers have evolved to use cryptocurrencies in their operations and are increasingly facilitated by new developments such as decentralised exchanges which allow exchanges without any Know Your Customer requirements. It is likely that high-privacy cryptocurrencies will make the current mixing services and tumblers obsolete."[563]

Furthermore, the mining aspect of cryptocurrencies has generated a new form of cybercrime. According to Europol's 2018 Internet Organised Crime Threat Assessment, 'cryptojacking' is an emerging cybercrime trend whereby internet users' bandwidth and processing power are exploited to mine cryptocurrencies.[564]

A key feature of cryptocurrencies is that they create opportunities for trusted transactions between distant parties without the need for a third-party verifier or certification authority, in the traditional sense. Through a select combination of techniques, bitcoin and other cryptocurrencies have managed to overcome the 'double-spending' issue that has plagued earlier attempts at creating digital currencies.

At any rate, it is clear that the cryptocurrency landscape will continue to develop and change through many small steps, both via law[565] and via technology, but also though major leaps, as exemplified by the controversial and forthcoming launch of Facebook's Libra.[566]

3.3.5.2 No central body as focal point for jurisdiction?

Given the distributed nature of blockchain technology, it is often argued that there is no central body in control of it. Where this the case, it has implications for the question of jurisdiction. In such situations, the lack of a central controlling body removes some of the focal points frequently relied upon for claims of jurisdiction, such as the place of incorporation or establishment.

Yet, despite the distributed nature of blockchain technology, the absence of a central authority is not a necessity. In fact, for several key uses of blockchain technology, a central body with some degree of control is essential. This would be the case in situations where a population's health records are stored on a blockchain. Presently, at least, it seems unimaginable that the relevant authority responsible for the health records could completely abdicate its responsibilities. Importantly, as one interviewed expert noted, the introduction of intermediaries in the blockchain environment activates traditional jurisdictional issues and connection points.

> "The introduction of intermediaries in the blockchain environment activates traditional jurisdictional issues and connection points."

3.3.5.3 Smart contracts

While cryptocurrencies, and particularly bitcoin, have attracted most of the attention around blockchain uses, blockchain-based smart contracts are discussed with increasing frequency. The term 'smart contract', however, dates back at least to 1994.[567]

A smart contract is a computerized transaction protocol that satisfies all ordinary criteria for being a contract (e.g., it must be concluded between two or more parties) and executes the terms of a contract so that once the smart contract has been concluded, its implementation does not require any direct human involvement.

There are no obstacles to such contracts being executed across borders. In fact, due to their self-executing nature, smart contracts may be particularly useful in cross-border transactions, as they avoid any uncertainties associated with enforcement.

---

563. Europol. (2018). *Internet Organised Crime Threat Assessment 2018*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf, p.8.

564. Europol. (2018). *Internet Organised Crime Threat Assessment 2018*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf, p.8.

565. Consider e.g. Mexico's Fintech law. See: Kurc, C. & Portilla, A. (2019, May 10). Mexico: Fintech 2019. *International Comparative Legal Guides*. Retrieved from https://iclg.com/practice-areas/fintech-laws-and-regulations/mexico.

566. *Libra White Paper*. Retrieved from https://libra.org/en-US/white-paper/.

567. Szabo, N. (1997). The idea of smart contracts. *Wayback Machine*. Retrieved from http://web.archive.org/web/20140406003401/szabo.best.vwh.net/idea.html.

3.3.6

Digital issues in international and regional trade agreements

With the online environment being a central component of commercial life, both domestically and internationally, it is only logical that digital issues would arise in international trade negotiations. Indeed, with the growth of the digital economy, digital issues will only increase in importance in such negotiations. For example, cross-border trade in services that may be carried out online is increasing and expanding into areas that have traditionally been viewed as domestic activities. As the World Trade Organization (WTO) has noted, services such as banking, health and education that were largely limited to domestic activities are now increasingly internationally mobile thanks to electronic banking, tele-health or tele-education services.[568]

Considering this, it is natural that trade agreements would also cover digital issues. For example, several trade agreements – such as the Trans-Pacific Partnership (TPP)[569] – mandate that parties adopt and maintain a legal framework for e-transactions that is consistent with the principles of the UNCITRAL Model Law on Electronic Commerce, or the UN Convention on the Use of Electronic Communications in International Contracts.[570] Furthermore, the EU-Japan Economic Partnership Agreement concluded in April 2018 provides detailed rules on e-commerce,[571] and the newly signed United States-Mexico-Canada Agreement includes a chapter on digital trade, as well as restrictions on data localization policies.[572]

At the same time, with data protection enshrined as a fundamental right in the EU, and an implied fundamental human right in large parts of the world, any trade agreement that implicates personal data raises significant complexities. In recognition of this, some key trade agreements explicitly recognize the role of data privacy protection, and the WTO has categorically stated that "WTO has had nothing whatever to do with internet privacy".[573]

The General Agreement on Trade in Services (GATS) explicitly states that it does not prevent the adoption or enforcement of measures to protect the privacy of individuals in relation to the processing and dissemination of personal data, and to protect the confidentiality of individual records and accounts. The freedom for members to pursue such measures, however, is "subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services".[574] Restrictions on cross-border data flows may consequently be challenged based on the assertion that they amount to arbitrary or unjustifiable discrimination.

The impact that trade agreements will have on data privacy and other central rights for online activities remains a challenge. While fundamental rights are not absolute, and often need to be balanced with other fundamental rights, they are non-negotiable. Therefore, in the same way that the US would not negotiate away its First Amendment protection of free speech as part of a trade agreement, the EU will not negotiate away the right of data protection.[575]

As one interviewed expert stressed, including human rights issues in trade negotiations raises issues of transparency. While opaque trade negotiations may be defensible, or even natural, in the context of trade tariffs, they are not so when the matter under negotiation is the application of fundamental rights.

---

568. World Trade Organization. *The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines*. Retrieved from https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm.

569. Article 14.5.

570. World Economic Forum. (2017, October). *White Paper: Making deals in cyberspace: What's the problem?* Retrieved from http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf, at 8.

571. EU-Japan Economic Partnership Agreement (2018, April). Retrieved from http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684, Chapter 8 Section F.

572. United States-Mexico-Canada Agreement. (2018, November 30). Retrieved from https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

573. World Trade Organization. *The WTO and internet privacy*. Retrieved from https://www.wto.org/english/tratop_e/serv_e/gats_factfiction10_e.htm.

574. General Agreement on Trade in Services, Article XIV.

575. *European Parliament Resolution of 12 December 2017: Towards a digital trade strategy* (2017/2065(INI). Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0488+0+DOC+XML+V0//EN.

3.3.6.1 Digital protectionism

The term digital protectionism is often used to describe any activities aimed at controlling the internet (and in the context of trade, the internet economy) within state borders – typically with the effect of imposing restrictions on foreign parties entering the market. This can be done in a variety of ways, and under a variety of pretexts.

Both in literature and among interviewed experts, it has been suggested that the EU's GDPR was introduced, at least partly, as a protectionist measure. Had the EU wanted to avoid the GDPR coming across as protectionist, it could have done more, for example, to limit the GDPR's extraterritorial reach.

> "Data localization requirements may be seen as an aspect of digital protectionism and may spark trade-related debates on the highest level."

Furthermore, data localization requirements may be seen as an aspect of digital protectionism and may spark trade-related debates on the highest level. For example, on October 12, 2018, two US senators sent an open letter to Indian Prime Minister Narendra Modi, asking that the Indian government soften its stance on data localization, and arguing that it is fundamental to the further development of digital trade.[576] In particular, the senators targeted a requirement from the Reserve Bank of India, the country's central bank, to store financial data within Indian territory.[577]

A further example of the intersection between international trade and digital protectionism can be found where sanctions are imposed to prevent cross-border trade. For example, on August 24, 2017, Apple reportedly removed popular apps used in Iran from its App Store, and issued a statement specifying that under the US sanctions regulations, the App Store cannot host, distribute or do business with apps or developers connected to certain US embargoed countries.[578] The removal of Iranian apps was met with criticism from the Iranian Telecommunication Minister, who announced his willingness to contest the decision.[579] Similarly, on May 15, 2017, Ukrainian President Petro Poroshenko signed a decree instructing local ISPs to block Russian websites, online media and social media platforms in the jurisdiction as part of a new round of economic sanctions against Russia, which annexed Crimea from Ukraine in 2014.[580] The block list notably included the search engine Yandex as well as the social media network VK, which is used by 20 million Ukrainians.[581]

In the long run, digital protectionism is likely to significantly undermine the international nature of the internet and potentially pose a threat to interoperability.

> "Digital protectionism is likely to significantly undermine the international nature of the internet and potentially pose a threat to interoperability."

3.3.6.2 Regionalization

Where regionalization creates entrenched and diverse legal and/or technical standards, it may become an obstacle to global solutions. At the same time, regional legal and/or technical standards may lay the groundwork for scalable solutions that may be transferred from a regional level to a global (or near-global) level. In this latter manner, regionalization may assist the establishment of global standards.

Trade policy has the potential to increase regionalization, but deeper forms of regional cooperation and coordination are an even stronger driving force. The EU is an obvious illustration of this, but there are many other examples, as well: the Asia-Pacific Economic Cooperation (APEC), the Association of South East Asian Nations (ASEAN), the African Union, the Community of Latin American and Caribbean States (CELAC), the Arab League and the Association of Caribbean States (ACS) and the Common Market for Eastern and Southern Africa (COMESA).

---

576. Kalra, A. (2018, October 13). Exclusive: U.S. senators urge India to soften data localization stance. *Reuters*. Retrieved from https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN.

577. Internet & Jurisdiction Policy Network. (2018, October). US Senators send letter to Indian PM to argue against central bank's data localization requirements. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7559_2018-10.

578. Internet & Jurisdiction Policy Network. (2017, August). Apple removes Iranian apps, arguing US sanctions make it necessary. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6239_2017-08.

579. Toor, A. (2017, August 25). Apple removes popular apps in Iran due to US sanctions. *The Verge*. Retrieved from https://www.theverge.com/2017/8/25/16201434/apple-iran-app-store-removal-sanctions-trump.

580. Roth, A. (2017, May 16). In new sanctions list, Ukraine targets Russian social-media sites. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/in-new-sanctions-list-ukraine-blocks-russian-social-media-sites/2017/05/16/a982ab4e-3a16-11e7-9e48-c4f199710b69_story.html.

581. Internet & Jurisdiction Policy Network. (2017, May). Ukraine blocks Russian internet platforms in new round of sanctions. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-5931_2017-05.

04

LEGAL AND TECHNICAL APPROACHES

—

EXPRESSION

SECURITY

ECONOMY

After a long period of relative inaction, there are now a myriad of legal approaches to addressing the cross-border legal challenges on the internet. Particularly over the past five years, both developing and industrialized countries have stopped procrastinating and taken a multiplicity of uncoordinated actions. Some jurisdictions have advanced with remarkable speed, setting global norms that compete, at least in part, with global norm-setting initiatives of other jurisdictions. Indeed, it may not be an exaggeration to speak of an ongoing race toward global norm setting between the EU, the US, China and, to a lesser extent, Russia.

States seek competitive advantages in the race to regulatory supremacy in a variety of ways. The initiatives range from political measures, such as building capacity and creating financial and security dependence among other countries, to the use of legal tools such as extraterritoriality and treaties. In this landscape, there is now a clear distinction between those who set norms, and those who largely adopt the norms set by others. Unsurprisingly, smaller and developing countries are almost exclusively at the receiving end.

> "Over the past five years, both developing and industrialized countries have stopped procrastinating and taken a multiplicity of uncoordinated actions."

Although laws offer some solutions, there is recognition that public-private standards, other forms of soft law and industry self-regulation may also offer solutions.

In addition, several technical solutions have been advanced, each with a substantial impact on the cross-border legal challenges on the internet. The aforementioned race towards global norm setting is playing out in this context, as well, with measures such as internet shutdowns, blocking and the forceful acquisition of innovation enablers making headlines in the news.

This Chapter outlines and analyzes a selection of major legal and technical approaches to solutions that experts emphasized in surveys and interviews, or that have gained particularly strong attention in the literature.

As one interviewed expert noted, the fact that the issues with which stakeholders now struggle are not new can either be viewed as a source of reassurance, or a cause for concern.

4.1

Major legal approaches to solutions

States take a wide range of legal approaches in the pursuit of what they perceive to be solutions to the cross-border legal challenges on the internet.

There is clearly an increased appetite for so-called 'takedown' and 'stay-down' orders from courts. There are also signs of a race to the highest potential fines – states are increasing the penalties they impose in order to prioritize adherence to their particular laws (over the adherence to competing legal frameworks imposed by other states).

Another emerging tool used to ensure enforceability of state law is so-called 'rep localization' – that is, laws requiring businesses to nominate a local representative within the state imposing the requirement. In addition, states are increasingly engaging in what may be described as jurisdictional trawling, whereby they make excessively broad claims of jurisdiction, giving them considerable discretion in deciding to whom to direct their enforcement efforts against. There is also a persistent, and perhaps growing, reliance on jurisdictional tests focused on so-called 'targeting'.

At the same time, however, there are some signs of restraint. While it remains a contested concept on the international level, comity and other calls for interest balancing are discernable on several levels. Furthermore, the matter of how states approach the scope of jurisdiction still hangs in the balance. Will the emerging practice of states seeking to give their judgments global effect become cemented? Or will a more nuanced approach prevail? This will be a key battleground in the coming years.

Finally, the extent to which terms of service and community guidelines, rather than law, shape online behavior remains a live issue.

As discussed in the introductory part of the Report (Chapter 1.5), attempts at finding legal approaches to solving the cross-border legal issues facing the internet are hampered by 'artificial regulatory challenges' – that is, contemporary frameworks and concepts are insufficient to successfully address these issues.

Overcoming such artificial regulatory challenges may require changes to traditional frameworks and concepts. But it also requires capacity building, which dovetails with the need for inclusiveness – a key issue to be considered in the context of approaches to solutions, and a recurring theme cited by surveyed and interviewed experts.

Both developing countries and many smaller states around the world are seen to be in the position of 'price-takers' – i.e., they must accept prevailing solutions and approaches from larger countries, without providing meaningful input. One interviewed expert suggested that this leads to a feeling of technological colonization, which causes resentment, particularly in countries with a colonial history.

While this point is raised in various contexts throughout the Report, it should certainly be considered in the examination of current approaches to solutions. It is important to assess not only how well these approaches work in the countries at the forefront of internet technologies, but also how they impact developing and smaller countries. Further, it is not enough to consider how well these approaches to solutions work today. It is also necessary to consider how they will work in the future, when the online environment is even more diverse.

4.1.1

Takedown, stay-down and stay-up orders by courts

Hundreds of millions of posts and hundreds of thousands of hours of videos are uploaded every day and made globally accessible on the major internet platforms. This greatly facilitates freedom of expression and provides access to information that enriches people's lives. As many interviewed experts noted, however, the internet mirrors the offline world, and so, alongside the content that educates, informs and entertains is content that offends, threatens and harms. This leads to legitimate concerns around the type of content available online.

> "In the absence of agreed substantive and procedural frameworks to handle the disparity of national laws, protecting freedom of expression and other human rights when dealing with abuses on the internet is a major transnational challenge."

In the absence of agreed substantive and procedural frameworks to handle the disparity of national laws, protecting freedom of expression and other human rights when dealing with abuses on the internet is a major transnational challenge. Content that is legal in one country may be illegal in another. Yet, "states that regulate or influence platforms often also, intentionally or not, shape speech rules that the platforms apply in other countries."[582]

Chapter 3 outlined major topical trends and highlighted the prevalence of orders requiring the takedown, delisting, deindexing, de-referencing, deleting, blocking, or removal of content. Such orders seem particularly common in the context of extremism and hate speech (Chapter 3.1.1), data privacy (Chapter 3.1.6), online bullying (Chapter 3.1.3), non-consensual distribution of sexually explicit media (Chapter 3.1.4), fake news and misinformation (Chapter 3.1.5), intellectual property (Chapter 3.3.1), child pornography (Chapter 3.2.1), fraudulent content (Chapter 3.2.1) and content amounting to a security risk (Chapter 3.2.4). In many countries, such orders are used to suppress political dissent, restrict freedom of expression, restrict freedom of religion and impose religiously motivated content restrictions.

On August 20, 2018, Apple announced[583] that it had removed 25,000 illegal gambling apps from its Chinese App Store, after being criticized by the Chinese media for failing to restrict access to the apps.[584] On July 4, 2018, the Indonesian Minister of Communications and Information announced that the Chinese video app Tik Tok was banned in the country because it contained pornography, inappropriate content and blasphemy.[585] On July 11, 2018, the Ministry stated[586] that the ban had been overturned, after the platform agreed to censor the 'negative content'.[587] This followed the Indonesian government blocking access to Tumblr in March 2018.[588]

On June 22, 2018, the South Korean internet content regulator (Korea Communications Standards Commission - KCSC) announced that Tumblr had agreed to better monitor illegal adult content on its platform.[589] The KCSC had demanded that Tumblr act on illegal adult content in September 2017 and the company refused, arguing that it was subject to the laws of the US, where it is based, leading the regulator to threaten a ban of the platform in the country.[590]

As this South Korean example illus-

---

582. Keller, D. (2019, January 29). Who do you sue? State and platform hybrid power over online speech. *Aegis Series Paper No. 1902*. Retrieved from https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf, p. 7.

583. BBC News. (2018, August 20). *Apple 'pulls gambling apps from China App Store'*. Retrieved from https://www.bbc.com/news/business-45243271.

584. Internet & Jurisdiction Policy Network. (2018, August). Apple removes gambling apps from Chinese App Store. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7260_2018-08.

585. Silviana, C. (2018, July 4). Indonesia bans Chinese video app Tik Tok for 'inappropriate content'. *Reuters*. Retrieved from https://www.reuters.com/article/us-indonesia-bytedance-ban/indonesia-bans-chinese-video-app-tik-tok-for-inappropriate-content-idUSKBN1JU0K8?feedType=RSS&feedName=technologyNews.

586. Silviana, C. & Potkin, F. (2018, July 11). Indonesia overturns ban on Chinese video app Tik Tok. *Reuters*. Retrieved from https://www.reuters.com/article/us-indonesia-bytedance/indonesia-overturns-ban-on-chinese-video-app-tik-tok-idUSKBN1K10A0.

587. Internet & Jurisdiction Policy Network. (2018, July). Indonesian authorities ban Chinese video app Tik Tok over pornography and blasphemy. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7189_2018-07.

588. Internet & Jurisdiction Policy Network. (2018, March). Indonesia blocks access to Tumblr after the platform fails to remove inappropriate content. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6888_2018-03.

589. Mu-Hyum, C. (2018, June 22). Tumblr to cooperate with Korean authorities to monitor porn. *ZD Net*. Retrieved from https://www.zdnet.com/article/tumblr-to-cooperate-with-korean-authorities-to-monitor-porn/.

590. Internet & Jurisdiction Policy Network. (2018, June). Tumblr agrees to better monitor illegal adult content in South Korea, says regulator. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7073_2018-06.

trates, failure to monitor and/or block content may result in threats to ban the service in question. And as discussed in Chapter 4.2.5, on some occasions, such bans are actually introduced.

In December 2018, it was reported that Russian telecommunications regulator *Roskomnadzor* fined Google 500,000 rubles (about 6,500 euros) for failing to comply with a requirement to remove entries from its search results.[591] Roskomnadzor again reportedly fined Google in July 2019[592] and in August 2019 demanded Google to stop advertising 'illegal' mass events on YouTube.[593] In fact, Russia is particularly active in pressuring internet intermediaries to remove content. On December 13, 2018, Twitter published its transparency report for the first half of 2018, highlighting an 80% increase in global requests for removal of content, with 87% of requests originating from Russia and Turkey.[594] And on September 9, 2018, it was reported[595] that YouTube had complied with a request from Russian officials to remove videos published by Russian dissident Alexei Navalny, as they were illegal under the country's election laws.[596]

Such extreme diversity in the underlying issues that may lead to orders to takedown, delist, deindex, de-reference, delete, block, or remove content makes it difficult to discuss such orders divorced from the underlying substantive law, leading to the order in question.

> "There is increasing attention directed at both stay-down orders and stay-up orders."

There is increasing attention directed at both stay-down orders and stay-up orders. The former is the stronger of the two trends, with a shift from content restrictions to content moderation and proactive detection. For example, at the time of writing, an ongoing matter before the CJEU (Case C-18/18) involves an Austrian politician who sought to make Facebook Ireland Ltd takedown unfavorable comments about her.[597] The CJEU was also asked to consider whether Facebook may be ordered to remove identically worded items of information, as well as information with an equivalent meaning. The Austrian politician in question is seeking to ensure that Facebook is forced to monitor content by continuously remove postings of the unfavorable comments made about her, including identically worded items of information and information with an equivalent meaning. The politician seeks these measures to be implemented worldwide.

On October 13, 2017, the Constitutional Court of Colombia ordered Google to delete a blog hosted by Google's Blogger.com, on the grounds that an anonymous post falsely claimed that an individual was guilty of fraud.[598] The Court also ruled that Google had to delete any future blog making the same defamatory allegations against the claimant. Moreover, the Constitutional Court asked the Ministry of ICT to introduce a new regulation to better protect the rights of Internet users.[599]

In 2017, an Australian court took the far-reaching step of ordering Twitter to apply filtering, or checking, to ensure that the information in dispute is either not posted or, if it is posted, removed.[600] The Court did not regard it as unreasonable that this stay-down order would extend to future tweets (regardless of topic) and future accounts held by any person or persons who use one or more of the offending accounts.[601] This is an extraordinary step, in that it imposes an obligation on

---

591. Internet & Jurisdiction Policy Network. (2018, December). Russia: Regulator fines Google 500 000 rubles for failing to remove search entries results. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7728_2018-12.

592. Internet & Jurisdiction Policy Network. (2019, July). Russia fines Google for failing to remove links for search results. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-8298_2019-07.

593. Internet & Jurisdiction Policy Network. (2019, August). Russia demands Google stop advertising illegal protests on YouTube. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoicnVzc2lhIiwiZnJvbSI6IjIwMTItMDliLCJ0byI6IjIwMTktMDgifQ==.

594. Internet & Jurisdiction Policy Network. (2018, December). Twitter publishes transparency report, showing sharp increase in public authorities' request for content removal. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7733_2018-12.

595. Bennetts, M. (2018, September 10). Russian police arrest hundreds protesting against Putin pension plan. *The Guardian*. Retrieved from https://www.theguardian.com/world/2018/sep/09/google-pulls-youtube-ad-by-putin-critic-alexei-navalny.

596. Internet & Jurisdiction Policy Network. (2018, September). YouTube complies with Russian request to remove dissident's videos. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7468_2018-09.

597. Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=202866&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4855084. For an in-depth discussion of the freedom of speech implications of this matter see: Keller. D. (2019). *Dolphins in the net: Internet content filters and the Advocate General's Glawischnig-Piesczek v. Facebook Ireland Opinion*. Retrieved from: https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-AG-Analysis.pdf.

598. John William Fierro Caicedo v Google Inc. and others. T-063A / 17. Retrieved from http://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm.

599. Internet & Jurisdiction Policy Network. (2017, October). Colombian Constitutional Court rules that Google must delete a Blogger.com blog that contained defamatory statements. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6369_2017-10.

600. X v Twitter Inc [2017] NSWSC 1300. Retrieved from http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html, para 36.

601. X v Twitter Inc [2017] NSWSC 1300. Retrieved from http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html, para 37.

a foreign company to ensure a lifetime ban on potentially foreign persons from using the company's platform for expression on any subject matter. The order is even more remarkable considering the seemingly weak jurisdictional connection to Australia.[602]

Examples such as Case C-18/18 before the CJEU, and the Supreme Court of New South Wales decision against Twitter, bring attention to the significant implications of stay-down orders as compared to takedown orders. While the weakness of takedown orders is obvious, in that the offending content may be uploaded again, stay-down orders have tremendous implications for freedom of expression – the impact of preventing the publication of content is very different to the impact of punishing the publisher of the content. For example, if content publication is prevented, there can be no public scrutiny of its potential value and legitimacy. Furthermore, the high volume of manual labor involved in content monitoring incentivizes internet platforms to automate content filtering. All this has the potential to make such automated filtering accurate, but not flawless.

Whether automated or not, content filtering gives rise to important issues of transparency, due process and the lack of an appeals processes. On a more fundamental level, it gives rise to questions around the distribution of rights and duties between the private and public sector, and may be seen as a privatization of state prerogatives.

Stay-up, or 'must carry', orders have so far gained less attention and have been pursued to a lesser degree.[603] Such orders typically require internet platforms to reinstate content that has been taken down, delisted, deindexed, de-referenced, deleted, blocked, or removed.

To date, stay-up orders have been primarily discussed in the context of US, German and Brazilian law. Where such orders have been sought under US law, they have failed:

> "Two dozen or more plaintiffs have tried suing platforms for taking down their posts or accounts, and the platforms have won every case. For starters, platforms' Terms of Service and statutory immunities under CDA 230 protect them from having to host speech they disagree with. More importantly, courts have consistently held that platforms' own First Amendment rights protect them from laws that would force them to host or index content against their will. That means that even the must-carry legislation that some politicians have threatened to pass probably wouldn't survive a Constitutional challenge."[604]

By contrast, courts in both Brazil and Germany have ordered internet platforms to reinstate content that the platforms determined to violate their community guidelines.[605] Orders such as these have, at least, as great a potential to create conflicts of law as do takedown orders. A scholar who has studied stay-up/must-carry issues in detail pointed to the need for courts to find doctrinal tools to decouple the must-carry issue from the global takedown issue (discussed in Chapter 4.1.7).[606]

A significant recent development unfolded in a December 4, 2018 judgment, where the European Court of Human Rights ruled that the freedom of expression of a news portal linking to defamatory statements had been infringed by an order from Hungarian courts to remove those links.[607] The Court argued that it could not agree with the domestic courts' approach, which equated the mere posting of a hyperlink with the dissemination of defamatory information, automatically imposing liability for the content itself.[608]

One of the Internet & Jurisdiction Policy Network's three thematic Programs – the Content & Jurisdiction Program – is developing solutions for how to manage globally available content considering the diversity of local laws and norms applicable on the internet.

---

602. Svantesson, D. (2017, November 14). Sydney to be become the internet content blocking capital of the world? *LinkedIn*. Retrieved from https://www.linkedin.com/pulse/sydney-become-internet-content-blocking-capital-world-svantesson/.

603. See, however: Keller, D. (2019, January 29). Who do you sue? State and platform hybrid power over online speech. *Aegis Series Paper No. 1902*. Retrieved from https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf.

604. Keller, D. (2018, September 13). Why DC Pundits' must-carry claims are relevant to global censorship. *The Center for Internet and Society*. Retrieved from http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship.

605. Masnick, M. (2018, September 7). German Court tells Facebook it can't delete comments, even though German law says it must delete comments. *Tech Dirt*. Retrieved from https://www.techdirt.com/articles/20180907/00455240595/german-court-tells-facebook-it-cant-delete-comments-even-though-german-law-says-it-must-delete-comments.shtml; http://www.omci.org.br/m/jurisprudencias/arquivos/2018/tjsc_00004474620168240175_06022018.pdf.

606. Keller, D. (2018, September 13). Why DC Pundits' must-carry claims are relevant to global censorship. *The Center for Internet and Society*. Retrieved from http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship.

607. European Court of Human Rights. Case of Magyar Jeti Zrt v Hungary (2018, December 4). 11257/16. Retrieved from https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-187930%22%5D%7D.

608. Internet & Jurisdiction Policy Network. (2018, December). ECHR rules that order to remove hyperlinks to defamatory statements infringe on news portal's freedom of expression. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7737_2018-12.

CONTENT
& JURISDICTION PROGRAM

Stakeholders in the Internet & Jurisdiction Policy Network work together in three policy Programs: the Data & Jurisdiction Program, Content & Jurisdiction Program, and Domains & Jurisdiction Program. The Programs allow members to informally coordinate policies and jointly develop proposals for operational Norms, Criteria and Mechanisms. The Content & Jurisdiction Program currently focusses on cross-border content moderation and restrictions with the objective of addressing applicable substantive norms, including the interplay between agreed international and regional human rights, national laws, and companies' community guidelines; the respective obligations of states and the respective responsibilities and protections of other actors, including the identification of allegedly illegal content; decision-making, standards and procedures, including the escalation path for individual decisions and appeal mechanisms; legitimate purposes, necessity and proportionality regarding the geographic scope of restrictions, and the necessary due process and transparency standards that should be applied across borders. Participants in the Program are focused on the following matters:[609]

- Standards – Addressing conflicts of different substantive norms to identify allegedly illegal content and determining the relationship/hierarchical nature of the relationship.
- Convergence – Level of global convergence achievable or desirable in such definitions.
- Response time – Appropriate reaction delays by intermediaries after reception of notices.
- Decision-making – The architecture of decision-making and the role of different types of state and non-state actors (including intermediaries, governments, courts, regulators and individuals that file requests).
- Algorithms – Appropriate combination of algorithmic tools and human review considering the limits of algorithmic tools.
- Procedural Standards – Procedural standards assessing the legality of content: assessment standards, assurance and verification, roles and remedies.
- Geographic scope – Situations, if any, that could, as a matter of exception from local filtering, justify global restrictions, including measures that address contradictory actions by different states.
- Transparency – Expanding existing efforts and strengthening coordination among them.
- Request formats – Documenting and circulating what proper government requests should contain.
- Notification – Handling of notification of users and their capacity to object.
- Remediation – Mechanisms for the prompt restoration of abusively restricted content.
- Types of content – Characteristics of content including intention and possible effects; determining appropriate measures for addressing different types of content.
- Types of actors – Roles and responsibilities.

---

609. 2nd Global Conference of the Internet & Jurisdiction Policy Network. (2018, February 26-28).*Ottawa Roadmap*. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf, at 8-9.
For the latest work plan, see 3rd Global Conference of the Internet & Jurisdiction Policy Network. (2019, June 3-5). *Berlin Roadmap*. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/Berlin-Roadmap-and-Secretariat-Summary-3rd-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf.

4.1.2

Race to the highest potential fines

The prospect of imposing high potential fines is a powerful regulatory weapon. A state threatening high fines is likely to attract media attention, which helps raise awareness of the law in question. More importantly, the higher the potential fines are for non-compliance, the greater the 'business incentive' is for ensuring compliance. This is particularly important in cases where the object of the regulation – such as a multinational business – is subject to competing regulation from another state, or other states. For example, a business caught by conflicting laws may opt to abide by the law of the state threatening the highest fines, at the expense of not abiding by the law of another state with lower fines.

Against this backdrop, it is unsurprising to see something of a race to highest potential fines. In November 2018, for example, it was reported[610] that the Russian government was considering amending a 2017 legal requirement that search engines remove links to banned websites from search results, in order to increase the maximum fines for non-compliance from 700,000 rubles (about €9,000) to 1% of a company's local revenue.[611]

Further, the tech industry is facing increasingly high fines in the field of competition law (antitrust law) both in the US and in the EU.[612]

On November 6, 2018, the Parliament of Mauritius adopted[613] amendments to the country's Information and Communication Technologies Act (ICTA), which aim to regulate and curtail harmful and illegal content and activities perpetrated via any information and communication service – including telecommunication services – through an increase in penalty and term of imprisonment for offenders.[614]

In the data privacy field, it can be noted that India's proposed data privacy bill includes fines up to approximately US$ 2.7 million or 4% of a company's global turnover,[615] Australia is seeking to increase its penalties,[616] and reference to the high potential fines under the EU's GDPR was made in Chapter 3.1.6.1. But the fines of up to €20 million, or 4% of the total worldwide annual turnover, envisaged under the GDPR is dwarfed by the threat of fines of up to 10% of the offending party's annual turnover found in Trinidad and Tobago's Data Protection Act 2011 (s. 69). In July 2019, Facebook reached a US$5 billion settlement with the Federal Trade Commission in relation to violations of consumers' privacy.[617]

The risk of high fines – a significant barrier for SMEs

Some interviewed experts emphasized that the risk of high potential fines is a significant barrier for SMEs, given that their access to sophisticated legal advice on complex legal issues and the associated compliance is often limited.

---

610. Torrent Freak. (2018, November 29). *Google, Facebook, VPNs and others risk huge fines under proposed law*. Retrieved from https://torrentfreak.com/google-facebook-vpns-and-others-risk-huge-fines-under-proposed-law-181129/.

611. Internet & Jurisdiction Policy Network. (2018, November). Russian regulator announces civil case against Google for failing to remove search results linking to permanently banned websites. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7678_2018-11.

612. Gupta, N,. (2019, July 24). Why DOJ Antitrust Review Is bad news for Facebook. *Market Realist*. Retrieved from https://articles2.marketrealist.com/2019/07/doj-antitrust-review-is-bad-news/.

613. Government of Mauritius (Port Louis). (2018, November 18). Mauritius: ICT Act amended to regulate and curtail harmful and illegal contents and activities. *All Africa*. [Press Release]. Port Louis. Retrieved from https://allafrica.com/stories/201811190697.html.

614. Internet & Jurisdiction Policy Network. (2018, November). Mauritius: Parliament passes amendments to ICT Act increasing penalties for spreading harmful and illegal content online. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7693_2018-11.

615. Coos, A. (2019, June 21). India's Personal Data Protection Bill: What we know so far. *Endpoint Protector*. Retrieved from https://www.endpointprotector.com/blog/indias-personal-data-protection-bill-what-we-know-so-far/.

616. Attorney-General for Australia Minister for Industrial Relations. (2019, March 2014). *Tougher Penalties to keep Australians safe online*. Retrieved from https://www.attorneygeneral.gov.au/Media/Pages/Tougher-penalties-to-keep-australians-safe-online-19.aspx

617. Federal Trade Commission. (2019, July 24). *FTC Imposes $5 Billion penalty and sweeping new privacy restrictions on Facebook*. [Press Release]. Retrieved from https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

The level of fines, while important, is only one of at least three central factors in this discussion. Another central factor is the degree of risk of actual enforcement. The threat of high fines may lack sting if it is not backed up with realistic enforcement processes – for example, via representative localization requirements (Chapter 4.1.3). In this context, one interviewed expert pointed to an emerging practice whereby courts order company funds to be frozen as a mechanism to ensure effective enforcement.

Yet, another central factor relates to the value of the market in question. If there is a practical risk of high fines being effectively enforced in a market that is of little value to the object of the regulation, such as a multinational business, that business may determine that the risks outweigh the benefits and simply abandon the market altogether. In this context, the complexity, clarity and certainty of the law in question is likely to affect the calculation. The combination of high fines and unpredictable, complex law creates higher risks that are more difficult mitigate.

In this environment, smaller countries – whether industrialized or developing – are at a competitive disadvantage because the value of their markets is smaller. Developing countries with weak enforcement tools at their disposal may be even further disadvantaged.

4.1.3

'Rep localization' – forced local representation

Recent years have seen a trend toward what may be called forced 'rep localization'. 'Rep localization' involves requirements mandating a foreign organization to maintain a physical representation in the state imposing the requirement. In this sense, there are parallels between 'rep localization' and 'data localization' – both are aimed at securing an enforcement advantage.

The GDPR and other EU regulations, for example, require foreign parties to designate, in writing, a representative in the EU under certain circumstances. This approach is self-enhancing, insofar as the more EU instruments that adopt this approach, the easier it is to justify in any given new context. The Proposal for an e-evidence Directive of the European Parliament and of the Council, for example, emphasizes that an obligation to designate a legal representative for non-EU service providers already exists in certain acts of EU law.[618]

Rep localization is clearly an onerous requirement for all foreign companies that would otherwise not have a physical presence in the EU, and the extent to which the EU is able to enforce this on a large scale remains to be seen. There is still the risk that arbitrary enforcement will undermine the scheme's legitimacy. There is also a practical matter to consider: how will a small-to-medium-sized foreign company make informed decisions in recruiting a trusted party to be its representative in the EU? And those in the EU who agree to assume this role face the risk of being held liable for the service provider's non-compliance.[619] Unless such a designated legal representative may be held fully accountable, the value of the entire system of forced rep localization should be questioned.

While the EU appears to be driving this development in the data privacy field at least, non-EU states have started to adopt the same approach, as well. For example, Thailand's proposed data protection law incorporates a rep localization requirement that is inspired by the EU, and potentially even broader.[620] The potential threat of jail sentences for data privacy violations in Thailand may further complicate the practical issues associated with finding trusted and willing local representatives. Like Thailand, other states around the world will likely follow the EU lead on this approach. The resulting regulatory web – with rep localization requirements in a large number of states – will be both difficult and costly to navigate.

Further, China requires a local representative to engage in online business, and on October 26, 2018, during a meeting of representatives from various Indian ministries and company representatives from Facebook, Google and WhatsApp, the Indian Home Ministry ordered the platforms to appoint local grievance officers as part of an effort to ensure the removal of objectionable or malicious content from public view.[621]

Vietnam's government, meanwhile, has asked Facebook to open an office within the country to comply with a 2018 cybersecurity law that amends requirements for the processing of Vietnamese users' personal data.[622] The law requires all platforms that

---

618. Proposed e-evidence Directive, Art 3.

619. Proposed e-evidence Directive, Art. 3(8).

620. Section 36(5), in September 2018 version.

621. Internet & Jurisdiction Policy Network. (2018, October). Indian government orders social media platforms to establish content monitoring system to track objectionable content. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7547_2018-10.

622. Nguyen, M. (2018, September 14). Vietnam urges Facebook to open office ahead of controversial cyber law. *Reuters*. Retrieved from https://www.reuters.com/article/us-facebook-vietnam/vietnam-urges-facebook-to-open-office-ahead-of-controversial-cyber-law-idUSKCN1LU13O?feedType=RSS&feedName=technologyNews.

offer services in Vietnam to remove offending content within one day of a request being filed, to store data within the country's territory, and to operate a local office.[623] The South Korean communications agency, Korea Communications Commission, has also announced its plans for 2019 which includes the development of 'Network Use Guidelines' requiring overseas operators to designate a local representative.[624]

Given the global nature of the internet, it is difficult to see how rep localization can be scalable. The EU approach may gain some acceptance among affected parties, since they only need to have representation in one EU Member State – a price that many online actors may be willing to pay – but how does this translate to the rest of the world? If Afghanistan, Argentina and Australia adopt the same approach, will it be worthwhile for internet companies to have representatives in each of those states, too?

One may respond to this concern by arguing that the way in which (largely US-based) tech companies interact with Afghanistan, Argentina and Australia is not the EU's problem; and such a response is not without merit. Yet, even to the extent that it works for the EU, rep localization is clearly not the solution for most other jurisdictions around the world. In fact, one could claim that the EU, and other bodies that actively seek to inspire legal developments in other states, should try to ensure that their approaches are scalable.

4.1.4

Jurisdictional trawling as a regulatory approach

As noted earlier, many states engage in what may be called 'jurisdictional trawling'; that is, they make broad claims of jurisdiction over internet activities – claims they cannot possibly back up with effective enforcement – and pursue only some of the internet activities over which they claim jurisdiction. Of the regulatory instruments discussed during interviews, Article 3 of the EU's GDPR (discussed in Chapter 3.1.6.1) is a prime, and frequently cited, example of this practice.

Brazil's Marco Civil is another strong example.[625] Under the adopted law, Brazilian data is considered to be subject to Brazilian jurisdiction, regardless of where it is physically stored. Article 11 of Marco Civil states that, "[i]n any operation of collection, storage, retention and treating of personal data or communications data by connection providers and internet applications providers where, at least, one of these acts takes place in the national territory, the Brazilian law must be mandatorily respected"[626]; and §2 adds that "[t]he established in Art. 11 applies even if the activities are carried out by a legal entity placed abroad, provided that it offers services to the Brazilian public or at least one member of the same economic group is established in Brazil."[627]

This approach – also referred to as 'regulatory overreaching' – has been widely criticized. It is arguably only defensible in situations where both the extraterritorial claim and the substantive law to which it relates can be justified as an appropriate demarcation of important societal values.[628] For example, broad claims of jurisdiction that cannot be backed-up with effective enforcement may nevertheless be justified if a state makes the claim as limited as the circumstances allow; and if the substantive law to which it relates is limited to an expression of societal values that align with international human rights standards and are central to the state in question.

Applying this to Article 3 of the EU's GDPR and Brazil's Marco Civil, it is clear that the respective jurisdictional claims are too broad, and some of the substantive rules (e.g., the GDPR's requirement of a data protection officer) are too burdensome.

Jurisdictional trawling leads to arbitrary enforcement, which interviewed experts described as a poor fit with the rule of law. It also contributes to the meta-trend of hyperregulation discussed in Chapter 2.2.2.

---

623. Internet & Jurisdiction Policy Network. (2018, September). Vietnamese government asks Facebook to open local office to comply with new cybersecurity law. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7456_2018-09.

624. Internet & Jurisdiction Policy Network. (2019, March). South Korea proposes the formulation of new Network Use Guidelines. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoic291dGgga29yZWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9.

625. Internet & Jurisdiction Policy Network. (2014, March). Brazilian congress approves Marco Civil Bill. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-4980_2014-03.

626. Internet & Jurisdiction Policy Network. (2014, April). Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04.

627. Internet & Jurisdiction Policy Network. (2014, April). Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04.

628. See further: Svantesson, D. (2017). *Solving the internet jurisdiction puzzle*. Oxford, United Kingdom: Oxford University Press, pp. 132-141.

4.1.5

Targeting/directing activities/doing business/'effects doctrine'

There is widespread recognition that a state may have jurisdiction resulting from activities initiated beyond its borders, in cases where the activities have a substantial connection to that state – e.g., by targeting consumers in that state, or causing harm there. This thinking is variously discussed in terms of 'targeting', 'directing activities', 'doing business' or, in the context of public international law, as the 'effects doctrine' (for convenience, it is referred to as the 'targeting test' below).

One early example of the targeting test expressly applied in the internet context is found in a 2002 US domestic internet defamation case. In *Young v. New Haven Advocate*[629], two newspapers based outside Virginia published articles, in part, discussing the conduct of residents of Virginia. The articles were available both offline and online. Despite this, the US Court of Appeals for the Fourth Circuit concluded:

> "The newspapers did not post materials on the Internet with the manifest intent of targeting Virginia readers. Accordingly, the newspapers could not have 'reasonably anticipated being haled into court [in Virginia] to answer for the truth of the statements made in their articles'. Calder, 465 U.S. at 790 (quotation omitted). In sum, the newspapers do not have sufficient Internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them."[630]

Another early targeting case came before the Federal Court of Australia in *Ward Group Pty Ltd v Brodie & Stone plc*. In this case, Australia, together with several other countries, was listed in a 'drop down' country box as a destination to which products may be shipped from a foreign website, and prices could be obtained in Australian dollars. Despite this, the Court concluded that: "The website proprietors' advertising on the internet of products for sale was a marketing of those products to the world at large and I am not satisfied that it was a marketing that was specifically targeted or directed at, or was specifically intended to be acted upon by, consumers in Australia."[631]

Under this reasoning, targeting the whole world means targeting no state in particular. However, the fairness of a business selling to the world at large being seen to not be targeting any state is highly questionable where a business targeting a handful of states is caught by the targeting test of all of those states. In contrast, listing prices in a local currency that differs from what a business commonly uses is explicitly mentioned as a relevant indicator of targeting in the EU's targeting test, as articulated by the CJEU in the joined cases of *Hotel Alpenhof/ Pammer*.[632] This model has been transplanted into the EU's GDPR[633], as well as in the EU's proposed Directive and Regulation on e-evidence.[634]

The fact that the targeting test is part of instruments already being copied in other legal systems suggests that it will now spread further. For example, the targeting test is now found in data protection proposals in Argentina and Thailand, which have both adopted the GDPR's approach.

> "whether or not a website has targeted a particular state must be determined on a case-by-case basis, and such an assessment invariably involves a high degree of arbitrariness."

Despite its widespread recognition, the targeting test is controversial due to the difficulty in ascertaining what amounts to targeting. For example, whether a website has targeted a particular state must be determined on a case-by-case basis, and such an assessment invariably involves a high degree of arbitrariness. Thus, the practical difficulties in ensuring a consistent application of the targeting test results in unpredictability for the parties. This undermines the value of the targeting test or creates an insurmountable obstacle to its effective use. After all, it is not only exorbitant jurisdictional claims that are problematic, but arbitrary jurisdictional claims, as well.

---

629. 315 F 3d 256 No. 01-2340 (13 December 2002).

630. Young v. New Haven Advocate 315 F 3d 256 No. 01-2340 (13 December 2002), at 7.

631. Ward Group Pty Ltd v Brodie & Stone plc (with Corrigendum dated 19 May 2005) [2005] FCA 471, para 37.

632. Joined Cases C-585/ 08 Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and C-144/ 09 Hotel Alpenhof GesmbH v Oliver Heller. For a detailed discussion of CJEU case law on this topic in torts matters, see: Gillies, L. E. (2019, July 5). *Conceptualising special jurisdiction for receipt orientated torts on the Internet: Lessons from CJEU jurisprudence.* Retrieved from https://ssrn.com/abstract=3416218 or http://dx.doi.org/10.2139/ssrn.3416218.

633. Recital 23.

634. COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=ENhttps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN; and COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

In the 2018 UK case of *Argos*, the UK High Court held that the US corporation selling construction software (Argos Systems) was targeting consumers in the UK through the use of Google Ads, which misdirected UK consumers looking for the UK based retailer of the same name. Argos Systems received revenue from the volume of traffic. Despite this, Argos UK were ultimately unsuccessful in establishing an unfair advantage.[635] An alternative to the targeting test is the related, but less-frequently discussed, 'dis-targeting approach',[636] which obliges businesses to actively regulate the jurisdictions they serve. This approach presumes that businesses are targeting the world at large; but this presumption is rebutted in cases where a business shows that it has taken appropriately active, yet perhaps simple, steps to avoid the risk of engaging with users in states deemed 'undesirable' for exposure. The burden this presents could be outweighed by the greater degree of predictability it provides, relative to the targeting test.

4.1.6

A common focus on comity, but a lack of agreement

It is only natural for online activities to connect with multiple jurisdictions; indeed, that is the default position. As a result, states need to account for interests other than their own.

In international law, the concept of comity has long been used as a tool for accounting for the interests of other states; and several recent developments affecting cross-border legal challenges on the internet have brought the concept into greater focus. A comity analysis forms an important part of the US CLOUD Act, and interest balancing is central in, for example, the EU's proposed Directive and Regulation on e-evidence.[637] Comity considerations also played a central role in the case of *Microsoft Corp. v. United States*[638], heard in the US Supreme Court on February 27, 2018, as well as in the many *amicus briefs* filed in relation to that matter. The European Commission clearly embraced the role of comity in its *amicus brief*, proclaiming that:

> "Any domestic law that creates cross-border obligations—whether enacted by the United States, the European Union, or another state—should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of 'mutual regard to the spheres of jurisdiction' of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law."[639]

In the context of cross-border legal challenges on the internet, the concept of comity is an important reminder that even if a state making a claim of jurisdiction has a strong connection to, and interest in, the matter at hand, it must still consider the rights and interests of other states before ultimately deciding to claim jurisdiction.

One interviewed expert noted that colleagues in the US often talk about comity, but that there are other important tools in (private) international law, as well. While the concept of comity can be found in both international law and the laws of various states, it lacks a uniform definition. Such ambiguity is not always appreciated, and commentators sometimes seem to assume that the well-developed concept of comity in US law represents its understanding globally. As recently as 2005, however, the judges of the High Court of Australia stated that comity is "either meaningless or misleading", and "a matter for sovereigns, not for judges required to decide a case according to the rights of the parties".[640] Clearly, attitudes toward comity vary greatly. This is merely one example of confusion around this concept, and clearly illustrates the importance of ensuring a common understanding.

---

635. Burbidge, R. (2018, October 15). Argos goes to the Court of Appeal but leaves empty handed. *The IPKat*. Retrieved from http://ipkitten.blogspot.com/2018/10/argos-goes-to-court-of-appeal-but.html?m=1.

636. Svantesson, D. (2001, September/October). What should Article 7 – Consumer contracts, of the proposed Hague Convention, aim to accomplish in relation to e-commerce? *Computer Law & Security Report*, 17(5), pp. 318 – 325.

637. COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=ENhttps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN; and COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

638. Wikipedia. *Microsoft Corp. v United States*. Retrieved from https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States.

639. United States v Microsoft Corp. Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party. Retrieved from https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf, 7.

640. Gummow and Hayne JJ in Neilson v Overseas Projects Corporation of Victoria Ltd (2005) 223 CLR 331, para 90.

4.1.7

Scope of jurisdiction – local court orders with global implications

Any time a court orders an internet actor to block, delist, deindex, de-reference, delete, remove, or takedown content, it will need to consider whether to grant that order only in relation to publications in the state where the court sits, or to extend the order more widely – and perhaps even globally. This issue – 'scope of jurisdiction' or, perhaps, 'scope of remedial jurisdiction'[641] – is currently a key 'battle ground', where multiple high-profile legal disputes are currently unfolding.

Thus, scope of jurisdiction relates to the appropriate geographical scope of orders rendered by a court that has personal jurisdiction and subject-matter jurisdiction – as in the blocking, delisting, deindexing, de-referencing, deletion, removal, or takedown situations mentioned above. The same issue arises when a court determines the damage to be awarded for online publications. The court may award damages only in relation to the effects felt in the state where the court sits, or to extend the damages order to other states (perhaps even globally).

Scope of jurisdiction in relation to internet content is not a new issue, however, it has been largely overlooked until recently. As early as 1999, the Supreme Court of New South Wales (Australia) expressed the view that:

> "[a]n injunction to restrain defamation in NSW [New South Wales] is designed to ensure compliance with the laws of NSW, and to protect the rights of plaintiffs, as those rights are defined by the law of NSW. Such an injunction is not designed to superimpose the law of NSW relating to defamation on every other state, territory and country of the world. Yet that would be the effect of an order restraining publication on the internet."[642]

This type of judicial self-restraint seems less common today. Scope of jurisdiction has gained considerable attention in light of high-profile disputes such as the 2016 Supreme Court of Canada *Equustek* case[643] (see Chapter 3.3.1), the CJEU's 2017 judgment in *Bolagsupplysningen OÜ*[644] (see Chapter 3.1.2.1), the right to be forgotten – *Google France* – dispute (see Chapter 3.1.6.2), and the *Glawischnig-Piesczek* case[645] (see Chapter 3.1.2.1).

Yet, this issue seems to attract less attention in many other parts of the world. For example, in its decision in *Hassel v. Bird* in July 2018, the Supreme Court of California reversed an order by the Court of Appeals, thereby ensuring that platforms can continue to rely on the protection afforded under Section 230 of the Communications Decency Act.[646] Tellingly, neither the Supreme Court of California nor the Court of Appeals saw reason to address the international implications of the case, even though the plaintiffs sought the removal of every defamatory review published by the defendant from Yelp.com and anywhere else they appeared on the internet.[647]

While the CJEU cases discussing the issue of scope of jurisdiction have gained considerable attention in academic and policy discussions, decisions such as *Hassell v. Bird*, which involve implied claims of global scope of jurisdiction – e.g., through content removal with global effect – are virtually ignored in debates.

Among the Internet & Jurisdiction Policy Network's stakeholders, there is widespread concern about courts making excessively broad claims of scope of jurisdiction.

"Among the Internet & Jurisdiction Policy Network's stakeholders, there is widespread concern about courts making excessively broad claims of scope of jurisdiction."

641. Svantesson, D. (2017). *Solving the internet jurisdiction puzzle*. Oxford, United Kingdom: Oxford University Press, pp. 171-189.
642. Macquarie Bank Limited & Anor v Berg [1999] NSWSC 526, para 14. Compare, however, X v Twitter Inc [2017] NSWSC 1300. Retrieved from http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html (Discussed in Chapter 4.1.1).
643. Google Inc v Equustek Solutions Inc 2017 SCC 34.
644. Case C-194/16 Bolagsupplysningen OÜ Ingrid Ilsjan v Svensk Handel AB.
645. Case C-18/18 Glawischnig-Piesczek.
646. Hassell v. Bird 234 Cal. Rptr. 3d 867 (2018). Section 230(c)(1) of the Communications Decency Act states that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".
647. Hassell v. Bird 234 Cal. Rptr. 3d 867 (2018) at 4.

Content restrictions should be global under certain circumstances

Among surveyed experts, a majority (64%) took the view that content restrictions should be global under certain circumstances. 27% took the view that content restrictions should never be global, and only 9% argued that content restrictions should be global by default.

Surveyed experts were largely united in the view that global content restrictions are appropriate in relation to content that is universally unlawful, with a large number pointing to bans on child sexual abuse content, as an example of such content. As noted by several respondents, virtually all other forms of content are subject to differing laws and norms. Some, however, mentioned a few other areas, including content promoting terrorism, copyright infringing content and content calling for genocide, as areas with a relatively high degree of harmonization.

A few surveyed experts took the view that content restrictions should be global to deter platforms from pandering to repressive regimes by offering selective blocking, and so that users in free countries can see and challenge blocks. As noted by another surveyed expert, however, global content restrictions may lead to the adoption of the most restrictive approaches and challenging foreign blocking orders may prove difficult.

It also seems likely that already dominant states will have greater success in pursuing orders with global scope, compared to smaller and developing states. In this way, claims of global scope of jurisdiction from leading states may prevent developing states from setting their own agendas. For certain purposes, such as preventing the creation of havens for child abuse materials, this intervention from dominant states may be appropriate. In other contexts, it may be inappropriate.

Several comments also noted that the scope of jurisdiction ought to be determined based on the facts of an individual case. For example, one surveyed expert noted that global content restrictions are motivated, when it is clear that a non-global restriction would cause actual damage.

Several interviewed experts also commented on the issue of scope of jurisdiction for content restriction. One interviewed expert observed that some providers make regional or language-based decisions in cases where content restrictions only apply to regions, rather than countries or the world, or to content in certain languages.

Some interviewed experts expressed concerns about current trends in global content restrictions, with one positing that it might take a conflict of laws issue for this challenge to be treated as a priority to be resolved at a government level, rather than an academic issue. Another interviewed expert discussed the challenges in reaching a consensus on norms for certain content. This is particularly difficult in, from a global perspective, are grey areas such as hate speech and neo-Nazi content, but agreement could be reached on appropriate processes, at least.

To summarize the responses, the Internet & Jurisdiction Policy Network's stakeholders are generally of the view that:

1. Global content restrictions are justified for certain content, at least for child abuse materials.
2. Apart from such content, the violation of local law should not, by default, be met with global content restrictions.
3. The appropriate scope of jurisdiction for content restrictions is context-specific. One size does not fit all.
4. There is value in monitoring content restrictions in order to provide transparency and opportunities to challenge content restrictions.

These are important observations that will hopefully inform courts, as a coherent framework for scope of jurisdiction evolves.

In addition, structural improvements were suggested. One surveyed expert suggested that in order to enhance the good faith amongst jurisdictions, one option is to create a League of Judges, similar to Convention of 25 October 1980 on the Civil Aspects of International Child Abduction. The judges would then know each other previously, which strengthens their relations and the enforcement of the judicial decisions may be more effective.

4.1.8

Terms of service and community guidelines

Internet platforms, and the terms of service and community standards they impose on their users, have a tremendous impact on the regulation of internet content. Indeed, due to the number of terms of service and community standards to which internet users are exposed, people now enter into more contracts than ever before. More importantly, these contracts include choice of forum and choice of law clauses that point to foreign courts and foreign laws.

Some of the overarching meta-trends explored in Chapter 2 relate directly to internet platforms. Here, focus is placed on the terms of service and community standards as such, and the role they play for cross-border legal challenges on the internet.

Terms of service and community standards normally address matters such as content moderation policies, intellectual property matters, limitations of liability, and the use, sharing and protection of user data. Importantly, they often outline how to resolve potential disputes, as well. They may, for example, include clauses that specify what country's law should be applied in the case of a dispute, and in which court(s) litigation may be instigated. They may also nominate specific out-of-court dispute resolution mechanisms, such as arbitration, mediation, or some form of online dispute resolution.

Despite the lack of negotiations, and despite their unilateral imposition, terms of service and community standards are, from a legal perspective, contracts between internet platforms and their users. Bygrave has written at length on the central role that contracts play in internet regulation. He illustrates, for example, that Lessig's classic description of the four regulatory forces (law, code, market and norms)[648], which has guided and indeed dominated much thinking on internet governance, fails to account for the distinctive role of contracts.[649] This is significant as contracts, including terms of service and community standards, often have a more direct impact on the activities of internet users than does legislation.

Because terms of service and community standards are typically made between businesses and consumers, consumer protection law often affects the terms they can include, and how they may be enforced. For example – as noted in Chapter 3.3.2 on e-commerce, marketing restrictions and consumer protection – recent court decisions in Canada and the EU have hinted at a possible trend against upholding choice of forum and choice of law clauses in online agreements.

Although their future as tools for imposing choice of law and choice of forum selections remains unclear, there is no doubt that terms of service and community standards will continue to be an important tool for content moderation – and they will continue to impact cross-border legal challenges on the internet in that context. If the law leaves the matter to internet platforms, for example, they may use their terms of service and community standards to outline the scope of jurisdiction they see as appropriate and remove or block content based on the standards they have set.

Terms of service also play a central role in the context of domain names. From the top down, the allocation of domain names is guided by contractual arrangements in what has been termed contract-based transnational private regulation.[650] The dispute resolution process prescribed in the agreements with domain name registrants is often held up as an example of successful self-regulation.

Finally, while terms of service, as a regulatory tool, may be seen as a product and a modern reiteration of the idea of community standards and self-regulation that characterized the internet's early days, they do not necessarily encompass the libertarian ideals that colored community standards and self-regulation.

---

648. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, 113(506).

649. Bygrave, L.A. (2015). *Internet governance by contract*. Oxford, United Kingdom: Oxford University Press, pp. 4-5.

650. Mahler, T. (2019). *Generic top-Level domains – A study of transnational private regulation*. Cheltenham, United Kingdom: Edward Elgar Publishing; Bygrave, L.A. (2015). *Internet governance by contract*. Oxford, United Kingdom: Oxford University Press, p. 50.

4.2

Major technical approaches to solutions

Many of the legal issues that arise in the context of internet technology may also be solved through that same technology. This section describes and examines the role of a selection of particularly significant technical approaches to solutions impacting the cross-border legal challenges on the internet.[651] A theme uniting many of these technical approaches is that they focus on limiting access to content.

The first technical approach to solutions – the use of so-called geo-location technologies – is currently a major 'battle ground'. The survey carried out for this Report specifically addressed geo-location technologies and sheds light on a divergence of views of the Internet & Jurisdiction Policy Network's stakeholders. Other technical measures aimed at limiting access to content include:

- Content filtering on the national network level;
- Court ordered suspension, deletion, non-resolving, seizure and transfer in the context of the Domain Name System;
- Court ordered DNS blocking, IP Address blocking or re-routing and URL blocking in the context of the Domain Name System;
- Service shutdowns; and
- Internet shutdowns.

All these technical blocking measurers, at least in their current form, have the potential to be undermined, if not rendered useless, by the development of satellite-based internet connectivity such as the OneWeb project[652] and Iridium[653], which provide satellite-based broadband connectivity worldwide.

The trend of forced data localization requirements is also examined, and attention is given to the multifaceted impact of artificial intelligence.

Technological complexity poses an obstacle to finding useful technical approaches to solutions to the cross-border legal challenges on the internet. Therefore, as in the context of legal approaches to solutions, there is a need for capacity building on every level. Technical capacity building is needed among both internet users and SMEs, as well as administrators, law enforcement, courts, governments and other stakeholders. This need is particularly acute in developing countries, but it also exists at the highest levels in developed countries.[654]

---

651. In addition to those discussed here, surveyed experts pointed to a range of other technical measures that are of significance, but perhaps somewhat more indirectly so as far as internet jurisdiction issues are concerned. Examples include e.g. algorithmic content shaping and disabling 3rd party tracking cookies by default in browsers.

652. OneWeb. Retrieved from https://www.oneweb.world/.

653. Iridium. Retrieved from https://www.iridium.com/.

654. See e.g.: Farrell, H. (2018, December 5). Rudy Giuliani is Trump's cybersecurity adviser. He might want a refresher. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2018/12/05/rudy-giuliani-is-trumps-cybersecurity-adviser-he-might-want-a-refresher/?noredirect=on&utm_term=.603492432f39, and BBC News. (2018, November 15). *Japan's cyber-security minister has 'never used a computer'*. Retrieved from https://www.bbc.com/news/technology-46222026.

4.2.1

Geo-location technologies – sacrificing 'borderlessness' to safeguard regulatory diversity

While the internet's 'borderless' nature is one of its hallmark characteristics, geography – and the physical location of internet users – remains relevant for many purposes. For example, ascertaining the physical location of an internet user may help those providing targeted search results or advertising, as well as those seeking to engage in market segregation. Doing so may also assist law enforcement, help fraud prevention and enhance cybersecurity.

Geo-location technologies, and the information they provide, may be important for jurisdictional purposes, as well. They offer service and content providers the opportunity to tailor their offerings to comply with the laws applicable at an internet user's location. They also give the option to avoid contact with internet users from specified locations in order to avoid exposure to laws applicable at those locations.

Geo-location technologies are technical means for ascertaining the physical location of internet users. They are, therefore, diverse by definition, and include techniques such as reliance on IP addresses, Wi-Fi information, GPS information and triangulation. Today, the use of geo-location is most commonly discussed as 'geo-blocking', even though blocking is merely one function of geo-location technologies. Moreover, geo-location technologies appear to have overtaken the use of cc-TLD based content diversification.

Detailed discussions on the role geo-location technology may play in the internet jurisdiction date back to the first half of the 2000s.[655] In the well-known French *Yahoo! case* of 2000 (Chapter 3.1), the Court concluded that "it may be estimated in practice that over 70% of the IP addresses of surfers residing in French territory can be identified as being French."[656] Yet, in a contemporaneous Supreme Court of New South Wales case, the Court emphasized that there were "no means by which material, once published on the internet, could be excluded from transmission to or receipt in any geographical area."[657] Such opposing views of geo-location technologies – with some courts emphasizing the role of geo-location technologies and others ignoring it completely – persist today.

Several courts and legislators today take geo-location technologies for granted, and indeed emphasize the importance of their use. For example, in the September 2018 case *Plixer International Inc. v Scrutinizer GmbH*, a US court emphasized that the German corporation in question could have designed its site to not interact with US users. It also rejected the German corporation's claim that the court should not consider whether a defendant blocks access to its website since, in the view of the corporation, access-blocking software is an imperfect developing technology.[658]

The CJEU, however, has a long tradition of ignoring geo-location technologies.[659] As recently as 2017, both the Court and Advocate General Bobek emphasized "the ubiquitous nature of the information and content placed online on a website and the fact that the scope of their distribution is, in principle, universal."[660] This statement clearly ignores the role geo-location technologies may have in limiting the geographical distribution of online content.

This reasoning brings attention to a broader issue. In reaching their conclusions, both Advocate General Bobek and the Court relied upon an assessment of internet technology made in 2011. In deciding a case in 2017, a court should not be guided by a six-year-old assessment of the state of technology. Rather, when assessing geo-location technology accuracy rates, it is important to be aware that they are:

1. time-specific;
2. location-specific; and
3. context-specific.

Courts must consequently make such assessments on a case-by-case basis, and not be led astray by estimates made in earlier decisions, or in different contexts.[661]

In September-October 2019, the CJEU addressed two cases directly dealing with the role of geo-location technologies.[662] In his Opinions in those

---

655. At least in English, the first in-depth law journal article devoted to the topic of geo-location technologies is: Svantesson, D. (2004, Fall). Geo-location technologies and other means of placing borders on the 'borderless' internet. *John Marshall Journal of Computer & Information Law,* XXIII (1), 101– 39.

656. International League Against Racism & Anti- Semitism (LICRA) and the Union of French Jewish Students (UEJF) v Yahoo! Inc, County Court of Paris, interim court order of 20 November 2000. However, it would seem that one of the experts, Ben Laurie, later felt a need to explain his statement (B Laurie, An Expert's Apology (on file with author)).

657. Macquarie Bank Limited & Anor v Berg [1999] NSWSC 526, para 12.

658. Plixer International, Inc. v. Scrutinizer GMBH, No. 18-1195 (1st Cir. 2018), p. 14.

659. See e.g.: Joined cases C- 585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and C-144/09 Hotel Alpenhof GesmbH v Oliver Heller, as well as, Joined cases C-509/09 and C-161/10 eDate Advertising GmbH and Others v X and Société MGN Limited.

660. Case C-194/16 Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB, para 48.

661. See further: Svantesson, D. (2008). How does the accuracy of geo-location technologies affect the law? *Masaryk University Journal of Law & Technology,* 2(1), 11– 21.

662. Google France, and Case C-18/18 Glawischnig-Piesczek.

matters, Advocate General Szpunar emphasized the role of geo-location technologies.[663] As to the role of geo-location technologies, the CJEU in Case C-507/17 emphasized their use and concluded that: "it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name"[664]
At the same time, the use of geo-location technologies is severely restricted by an EU Regulation that applies from December 3, 2018, and which forms part of the EU's *Digital Single Market Strategy*.[665]
The Geo-Blocking Regulation seeks to address "unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market". It is noteworthy that the Regulation is justified primarily by reference to the ills of discrimination based on customers' nationality, place of residence or place of establishment; yet it targets geo-blocking which, by its very nature, cannot recognize nationality, place of residence or place of establishment. Location may merely serve as an unreliable proxy for nationality, place of residence or place of establishment.

The Geo-Blocking Regulation outlines three specific circumstances under which the use of geo-blocking cannot be justified:

- The sale of goods without physical delivery.
- The sale of electronically supplied services, other than those that primarily provide access to copyright protected works or other protected subject matter (including the sale of copyright protected works or protected subject matter in an intangible form).
- The sale of services provided in a specific physical location.[666]

The Regulation also bans blocking of access to websites and the use of automatic re-routing if the customer has not given prior consent.

> "It can be expected that the way the EU law develops on topic of geo-location will influence other jurisdictions."

The tension between the policy goals pursued by the Geo-blocking Regulation and those that led Advocate General Szpunar to emphasize the use of geo-location technologies is not limited to the EU context. It can be expected that the way the EU law develops on topic of geo-location will influence other jurisdictions.

Divergent stakeholder attitudes towards geo-location technologies

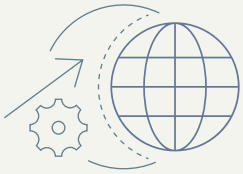
Surveyed experts were presented the statement that geo-location, used by internet platforms or content providers to block access to content from certain countries, is an effective tool for ensuring compliance with national law locally, without resorting to global delisting, removal, blocking, etc. Among those surveyed, 5% 'strongly agreed' with the statement, while 29.5% 'agreed'. Only 1% 'strongly disagreed', 29.5% 'disagreed', and 35% neither agreed nor disagreed.

This survey result was relatively equally distributed from a geographical perspective, though different stakeholder groups expressed a significant divergence in attitudes.
While stakeholders from academia and from civil society were predominantly positive about the role of geo-location, those from the technical community were overwhelmingly negative.
In the comments from surveyed experts, three recurring themes stood out. The first is that geo-location technologies can be easily bypassed. One respondent, for instance, noted that virtual private networks (VPNs) are far too prevalent, cheap, easy-to-use and effective for geo-location technologies to be a truly powerful technique for determining which users to block.

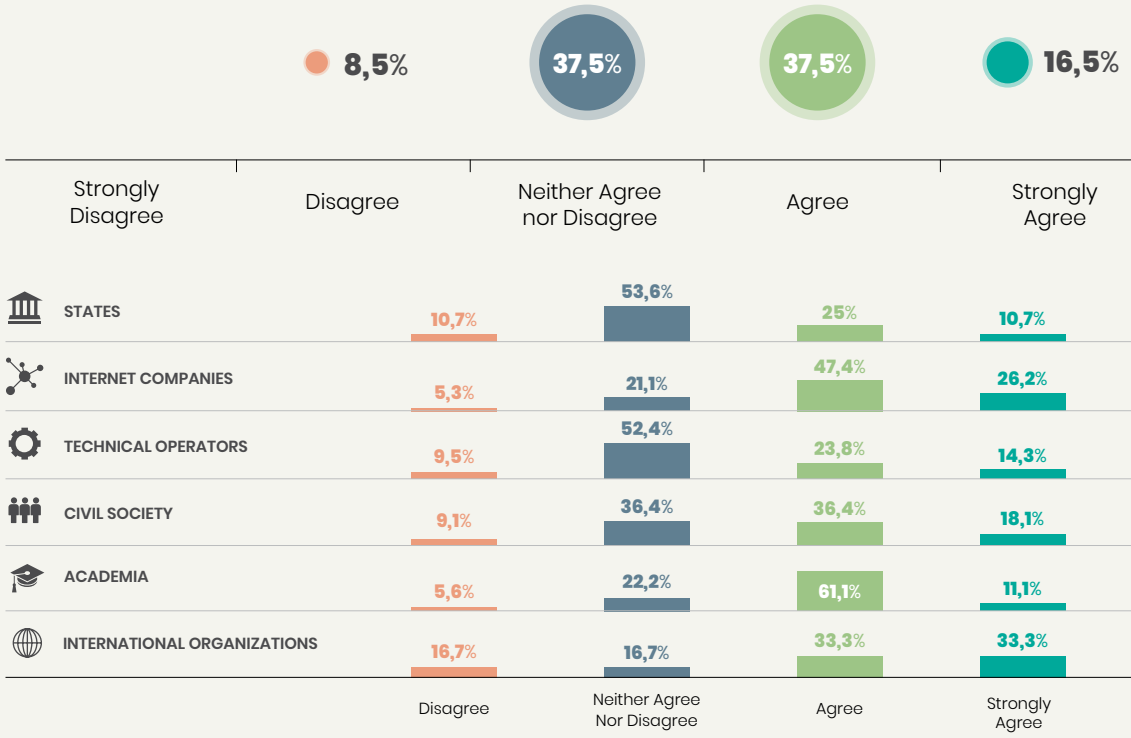
---

663. C-507-17 Google v CNIL. Advocate General Opinion. (2019, January 10). Luxembourg. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002en.pdf; C-18-18 Eva Glawischnig-Piesczek v Facebook Ireland Limited. Advocate General Opinion. (2019, June 4). Luxembourg. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=388718.
664. Case C-507/17 Google v CNIL, para 70.
665. European Commission. *Digital single market: Economy & society*. Retrieved from https://ec.europa.eu/digital-single-market/en/economy-society.
666. European Commission. *Digital single market: Geo-blocking*. Retrieved from https://ec.europa.eu/digital-single-market/en/policies/geoblocking.

INFOGRAPHIC 13



Are cross-border legal challenges on the internet a significant barrier for developing countries?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

VPNs and anonymizers – a 'double-edged sword'

VPNs and anonymizers are frequently discussed in the context of cross-border legal challenges on the internet. Their ability to cater for the circumvention of geo-location technologies has gained especially strong attention. They are also often discussed in the context of their ability to shield the actual identity and physical location of internet users in order to protect privacy.

One interviewed expert stressed the role of anonymity as a protector of human rights in authoritarian regimes. Technologies such as VPNs must, therefore, be evaluated not just as tools of circumventing geo-blocking, but as tools of free speech.

VPNs and anonymizers are truly 'double-edged swords' in that, while they can be used by criminals to avoid being brought to justice, they are also essential tools for human rights defenders in repressive regimes – and indeed, for the average internet user seeking to maintain a degree of privacy while connecting to a public Wi-Fi network.

In some parts of the world, such as Dubai, only state-licensed VPNs are allowed. Some countries ban VPNs altogether. For example, on November 1, 2017, for example, the Federal Law No. 276-FZ – which outlaws the use of VPNs and other technical tools to circumvent website access restrictions – entered into force in Russia.[667] The law forbids search engines from displaying results containing information about, or links to, blocked websites, and empowers the Russian

667. Federal Law No. 276-FZ. Retrieved from http://publication.pravo.gov.ru/Document/View/0001201707300002?index=0&rangeSize=1.

telecommunication regulator *Roskomnadzor* to require ISPs to identify owners of circumvention tools.[668] Furthermore, on March 31, 2018, a ban on non-state sanctioned VPNs entered into force in China.[669] The measure was announced in January 2017, and in July of that year, the Chinese Ministry of Industry and Information Technology (MIIT) ordered state-run telecommunication operators to block VPNs by February 2018. MIIT chief engineer Zhang Feng specified that foreign companies seeking to set up a cross-border operation for private use will need to set up a dedicated line for that purpose, which can be legally leased from the telecommunications import and export bureau.[670]

While it is correct that circumvention through VPNs undermines the accuracy of geo-location technologies, such circumvention typically requires intent. In other words, the use of circumvention tools ordinarily presupposes an awareness of what content can be accessed by using those tools. This severely limits the actual impact of VPNs in many cases.

One surveyed expert further emphasized the importance of distinguishing between the questions of technical efficiency on the one hand, and legal adequacy on the other. While describing geo-location as somewhat effective in a technical sense, this respondent took the view that geo-location technologies should be considered legally adequate, given overall considerations such as comity and the human rights margin of appreciation. This illustrates a difference in thinking among respondents, with some primarily thinking of the technical efficiency of geo-location technologies, and others focusing on the legal adequacy of such technologies. This could explain the difference in attitudes seen across different stakeholder groups.

A second recurring theme is that geo-location technologies may negatively impact freedom of expression online, and that internet users may not even be aware that their freedom of expression and access to information are affected.

The third recurring theme is that even though geo-location technologies are not a foolproof way for internet platforms to ensure compliance with local laws, they are still preferable to global delisting, removal and blocking in most circumstances.

In addition to these three main themes, surveyed experts commented that geo-location technologies must be applied carefully in order to limit the number of false negatives, and to avoid negatively affecting DNS performance. One surveyed expert also noted that while using geo-location technologies to block access to content from certain countries may work quite well for paid-for media content,[671] it imposes costs for most free content, and it is not clear who should cover these costs.

Ultimately, it is impossible to assess the desirability of geo-location technologies in a vacuum. Such a determination must instead be carried out as a comparative exercise, where advantages and disadvantages are compared to those of relevant alternatives. In comparing an internet grounded in an extensive use of geo-location technologies to an internet that is open, global and unrestricted, many may favor the latter. However, such a utopian internet does not exist today and has arguably never existed.

It, therefore, seems more realistic, and more relevant, to compare an internet grounded in an extensive use of geo-location technologies to one characterized by global blocking, removal and delisting based on claims of jurisdiction – in other words, an internet where the only content that remains online is that which offends no law anywhere in the world. In this latter comparison – as suggested in comments from surveyed experts – an internet grounded in the extensive use of geo-location technologies may perhaps be favored due to its potential to keep the world connected, while still allowing for regulatory diversity.

In the fields of data privacy and cybersecurity, it is common to speak of privacy-by-design and security-by-design, respectively. Looking to the future, perhaps an increase in appropriate use of geo-location technologies could be described as 'jurisdictional interoperability-by-design' – that is, jurisdictional interoperability, in the form of compliance with diverse and potentially conflicting local laws, that is more clearly incorporated into technical designs.

---

668. Internet & Jurisdiction Policy Network. (2017, November). Russian regulation outlawing the use of tools to circumvent access restrictions such as VPNs enters into force. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6552_2017-11.

669. Cadell, C. & Martina, M. (2018, March 30). Businesses, consumers uncertain ahead of China VPN ban. *Reuters*. Retrieved from https://www.reuters.com/article/us-china-vpns/businesses-consumers-uncertain-ahead-of-china-vpn-ban-idUSKBN1H612F.

670. Internet & Jurisdiction Policy Network. (2018, March). China: Ban on non-state sanctioned VPNs entered into force. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6891_2018-03.

671. For example, in the case of the GDPR fallout the non-European newspapers blocking European users (https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr) actually used geo-blocking measures with the argument, that the potential cost of being non-compliant would be considerably higher.

4.2.2

Content filtering on the national network level

Blocking and censorship have obvious and profound implications for the cross-border internet. They contribute to fragmentation and suggest that the internet is not as borderless as it may seem. Yet, compared to claims of global scope of jurisdiction made to ensure that content is blocked, delisted or removed on the internet as a whole, content filtering on the national network level has a more limited impact.

The geo-location technologies discussed in the above section should not be confused with content filtering on the national network level – the kind carried out, most famously, through the so-called 'Great Firewall of China'. By blocking access to selected foreign content and websites, the Great Firewall encompasses the legislative and technical restrictions that the Chinese government uses to regulate the internet domestically. Similar structures have been adopted and tested in several other states with repressive governments that hold hostile attitudes toward the type of freedom of expression that is enjoyed elsewhere.[672] In addition, there are efforts from Chinese companies to export part of the Great Firewall's functionality to other countries, not all of which have repressive governments.

4.2.3

Domain Name System: court ordered suspension, deletion, non-resolving, seizure and transfer

The domain name system (DNS), as an addressing system, is a neutral technical layer that is vital for the proper functioning of the internet. Nevertheless, cross-border requests for domain name suspension are increasingly sent to technical operators regarding alleged abusive content or activity on underlying websites.

From the requestors' perspective, the appeal of such requests is obvious – a domain suspension has, by definition, an instant global impact. At the same time, this potential for instant global impact means that requests for domain name suspension should only be considered when one can reliably determine that a domain is used with a clear intent of significant abusive conduct; only a particularly high level of abuse and/or harm could justify resorting to such a measure. Such requests must also be framed with extensive procedural safeguards for all parties involved. The protection of the core of the internet – including the DNS – is, and should be, a key priority. This undermines the use of domain name suspension requests as a tool to tackle abusive content or activity on underlying websites.

> "The protection of the core of the internet – including the DNS – is, and should be, a key priority."

To ensure protection of the DNS, it is important to have a strong understanding of the impacts of specific actions at the DNS level. Yet, interviewed experts noted that the DNS is poorly understood, and that its complexity is often underestimated. For example, there is a widespread failure to appreciate the different structures of both the generic Top Level Domains (gTLDs) and the country-code Top Level Domains (ccTLDs). This results in an under-appreciation of the fundamental distinctions between how the Internet Corporation for Assigned Names and Numbers (ICANN) structure, and national laws or authorities, apply to different entities receiving requests for domain name suspensions.

In a colorful observation, one interviewed expert noted that attempts at using the protocol layer to affect a desired outcome at the application layer is like seeking to prevent drug trafficking on highways by regulating asphalt manufacturers to slow down vehicles. The interviewed expert added that, although it is true that vehicles carrying drugs would be slowed down, drug couriers would find alternative modes of transport, while the harm done to other (innocent) vehicles would be extensive.

While capacity building takes place in this sphere, the domain architecture is becoming increasingly complex. This has occurred due to ccTLDs behaving like gTLDs, as well as the introduction of new gTLDs.

All actors are confronted with common challenges: to define when is it appropriate to act at the DNS level in relation to the content or behavior of a domain address, and to identify the respective roles that courts and so-called 'notifiers' should play. These matters are examined in one of the Internet & Jurisdiction Policy Network's three Thematic Programs.

---

672. Cimpanu, C. (2019, February 11). Russia to disconnect from the internet as part of a planned test. *ZD Net*. Retrieved from https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/.

DOMAINS & JURISDICTION PROGRAM

Stakeholders in the Internet & Jurisdiction Policy Network work together in three policy Programs: the Data & Jurisdiction Program, Content & Jurisdiction Program, and Domains & Jurisdiction Program. The Programs allow members to informally coordinate policies and jointly develop proposals for operational Norms, Criteria and Mechanisms. The Domains & Jurisdiction Program currently focusses on defining on a topic-by-topic basis under what strict conditions might interruption of a domain name without consent of the registrant be envisaged/acceptable; what actions should/would domain name operators be willing and able to exercise; what rules and procedures could help establish or enhance the credibility of notifiers' notifications (for information or action); and what possible mechanisms can help improve transparency in such processes.

The Domains & Jurisdiction Program's current work is based on the Ottawa Roadmap of the Internet & Jurisdiction Policy Network that produced concrete proposals for operational Norms, Criteria, and Mechanisms in 2019.[673] It addresses the following issues:

- Standards – Taxonomy and threshold levels for action relevant to each type of abusive behavior and content.
- Court orders – The role of court orders, including their territorial reach, their effectiveness regarding and their proportionality.
- Notifications – Criteria relevant to evaluate the credibility of a notification, with the source (i.e., the notifier) being only one element.
- Due Diligence – The procedures notifiers should ideally follow before sending out notifications, and the content of their requests.
- Procedural guarantees – Protections for registrants (notification and contradictory procedure, proportionality).
- Remediation – Appeal mechanisms and technical precautions that allow for remediation.
- Request validation – Options for certification of notifications.
- Liability – Potential protections for operators when proper due diligence is conducted.
- Transparency – Mechanisms to ensure appropriate transparency, including in relation to how operators deal with notifications, and how notifiers ensure due process prior to notification.
- Education – Accessible and high-quality information for lawmakers, courts and law enforcement to prevent unintended consequences of decisions, as well as for end users, who can play a crucial role in preventing abuse.
- Tools – Software and/or processes to enable effective, proportionate and scalable measures.

4.2.4

Domain Name System: court ordered DNS blocking, IP Address blocking or re-routing and URL blocking

DNS blocking is an approach that relates to the court-ordered suspension, deletion, non-resolving, seizure and transfer of domain names discussed above. A DNS blocking order typically requires one or several ISPs to implement a system that disables access to one or several 'target online locations'. This procedure is exemplified in a 2018 judgment of the Federal Court of Australia. In *Roadshow Films Pty Limited v Telstra Corporation Limited*, a group of ISPs was ordered to take steps to prevent access to a large number of websites. The court specified that to comply with this order, the ISPs would need to implement one or more of the following steps:

> "(a) DNS Blocking in respect of the Target Domain Names;
> (b) IP Address blocking or re-routing in respect of the Target IP Addresses;
> (c) URL blocking in respect of the Target URLs and the Target Domain Names; or
> (d) any alternative technical means for disabling access to the Target Online Location as agreed in writing between the Applicants and a Respondent."[674]

Much like court-ordered suspensions

673. 2nd Global Conference of the Internet & Jurisdiction Policy Network. (2018, February 26-28). Ottawa Roadmap. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/ Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf, at 10-11. For the concrete proposals , see: Internet & Jurisdiction Policy Network. *Domains & Jurisdiction Program Operational Approaches*. Retrieved from http://internetjurisdiction.net/Domains-Jurisdiction-Program-Operational-Approaches.
For the latest work plan, see 3rd Global Conference of the Internet & Jurisdiction Policy Network. (2019, June 3-5). *Berlin Roadmap*. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/Berlin-Roadmap-and-Secretariat-Summary-3rd-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf

674. Roadshow Films Pty Limited v Telstra Corporation Limited [2018] FCA 582, para 3.

and the deletion, non-resolving, seizure and transfer of domain names, this type of order is controversial. The risk of discrimination and over blocking is obvious, and there are clear issues of responsibility, remedy and redress. One interviewed expert brought attention to a high-profile case of over-blocking that occurred in 2016, when the French ISP Orange mistakenly blocked the traffic to Google, Wikipedia and several other websites for its 11 million landline customers.[675] These issues will be augmented in cases where blocking is supplemented by algorithms and artificial intelligence. Nevertheless, there are areas in which such orders may receive support. For example, one interviewed expert noted that requirements to block fraudulent URLs, or those that automatically install malware, should in fact be global.

"The risk of discrimination and over blocking is obvious, and there are clear issues of responsibility, remedy and redress."

4.2.5

Service shutdowns

Governments frequently threaten to shut down specific internet services, and on some occasions, those threats are actually carried out. Where this happens, and the service provider is a local business, the matter is largely domestic. However, cross-border impacts arise if the service provider is a foreign company, which often is the case. Situations where a domestic service provider is blocked may have trans-border dimensions, as well. Such a service, for example, may have users in other countries that are affected, and various international obligations may be implicated.

Yet, despite the serious implications of such measures, services are frequently blocked, and service shutdowns occur across the globe:

- **China** regularly blocks various services, and its censorship is particularly strict around dates of historical significance.[676] For example, the websites of 12 major international news outlets from five different countries were blocked specifically in the lead up to the 30th anniversary of the Tiananmen Square massacre.[677]
- In **July 2019**, the government of **Chad** lifted a 16 month ban on social media which the government stated was necessary for security reasons.[678]
- On **May 29, 2018**, Communications Minister of **Papua New Guinea**, Sam Basil, announced that the country would block access to Facebook for a month, in order to collect information to identify, filter and remove users that hide behind fake accounts, upload pornographic images, or post false and misleading information on Facebook. The Minister cited the 2016 Cyber Crime Act as the basis for the block and mentioned that the government was also "look[ing] at the possibility of creating a new social network site for PNG citizens with genuine profiles as well."[679]
- On **May 26, 2018**, **Egypt**'s top administrative court ruled that YouTube should be blocked for one month over 'The Innocence of Muslims', a 2012 anti-Islamic video that sparked protests in the Middle East upon its release.[680] A lower administrative had ordered the block in **2013**, after which the case was appealed until the May 26, 2018 ruling.[681]
- On **April 13, 2018**, a Russian court ordered that access to the messaging service Telegram be blocked in **Russia**, following

---

675. See further: Freedom House. (2017). *Freedom on the net 2017*. Retrieved from https://freedomhouse.org/report/freedom-net/2017/france.
676. Cook. S, (2019, June 24). China's Long, Hot Summer of Censorship. *The Diplomat*. Retrieved from https://thediplomat.com/2019/06/chinas-long-hot-summer-of-censorship/.
677. Van Graver. D, (2019, July 4). The "new era" of digital authoritarianism. *The Interpreter*. Retrieved from https://www.lowyinstitute.org/the-interpreter/new-era-digital-authoritarianism.
678. Nadjitan, D.N. (2019, July 14). Chad Lifts Ban on Social-Media Usage After More Than a Year. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-07-14/chad-lifts-ban-on-social-media-usage-after-more-than-a-year.
679. Internet & Jurisdiction Policy Network. (2018, May). Papua New Guinea announces month-long Facebook block over misinformation, adult content and fake accounts. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7038_2018-05.
680. Abdellah, M., Ahmed, H. & Atallah, M.S. (2018, May 26). Top Egypt court orders temporary YouTube ban over Prophet Mohammad video. *Reuters*. Retrieved from https://www.reuters.com/article/us-egypt-youtube/top-egypt-court-orders-temporary-youtube-ban-over-prophet-mohammad-video-idUSKCN1IR0FD.
681. Internet & Jurisdiction Policy Network. (2018, May). Egypt Supreme Administrative Court orders one-month block of YouTube over 2012 anti-Islamic video. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7049_2018-05.

the platform's repeated refusal to hand over its encryption keys to the FSB, the Russian security agency.[682] This was met with considerable opposition.[683] A few days thereafter, on **April 17, 2018**, *Roskomnadzor* requested that Google and Apple remove Telegram from their application stores. On the same day, the regulator announced that it had blocked millions of IP addresses belonging to Amazon Web Services and Google Cloud, in an attempt to block access to Telegram. This resulted in disruptions for other services, including Google's search engine and email service.[684]

- On **March 8, 2018**, the government of **Sri Lanka** ordered ISPs to temporarily block access to Facebook, WhatsApp and Instagram because they were spreading and amplifying hate speech amid violent protests in the country, according to a government spokesperson.[685] The ban was lifted a week later, after meetings between Sri Lankan authorities and representatives of the platform.[686] Social media and messaging apps were again temporarily blocked by the Sri Lankan government in **April 2019** to prevent misinformation and incitement of violence in the wake of terrorist attacks.[687]
- On **November 8, 2017**, the Ministry of Communications of **Indonesia** announced that it would launch, in **January 2018**, an automated system to flag and block websites or messaging services displaying pornography or extremist content.[688] The government also stated that it would summon executives of messaging services and search engines to demand that they moderate obscene content. The announcement followed the Indonesian government's threat to ban WhatsApp if it did not move to block obscene GIFs on its platform.[689] In **May 2019**, the Indonesian government temporarily restricted access to social media platforms including Facebook, WhatsApp and Instagram seeking to prevent misinformation and provocation following violent riots in Jakarta.[690]
- On **September 6, 2017**, it was reported that access to Facebook and WhatsApp was difficult in **Togo**, before all mobile internet was reportedly shut down.[691] After service was restored, WhatsApp was again blocked, as connection speeds slowed down on **September 19, 2017**. The internet access restrictions came amid intensifying anti-government protests in the country.[692]
- On **May 12, 2017**, the National Broadcasting and Telecommunications Commission (NBTC) of **Thailand** threatened to block Facebook unless the US-based company removed 130 'illegal' posts.[693] The demand came after the Thai Internet Service Provider Association (TISPA), which accounts for 95% of internet traffic in the country, purportedly requested that Facebook Thailand restrict access to content critical of the monarchy.[694]
- On **May 5, 2017**, a Turkish court in Ankara rejected an appeal by the Wikimedia Foundation against a blocking of Wikipedia in the jurisdiction.[695] On **April 29**, the Turkish telecommunications authority BTK announced that Wikipedia would be blocked through an administrative measure citing law no. 5651, which regulates online content in **Turkey**. After the blocking, the Turkish Communications ministry stated that Wikipedia had been part of a smear campaign against Turkey in the international arena. In their decision, the judges of the Ankara court were quoted as saying that while freedom of

---

682. MacFarquhar, N. (2018, April 13). Russian court bans Telegram app after 18-minute hearing. *The New York Times*. Retrieved from https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html.
683. Transparency International. (2018, May 16). *Russia: Telegram block leads to widespread assault on freedom of expression online*. Retrieved from https://www.transparency.org/news/pressrelease/russia_telegram_block_leads_to_widespread_assault_on_freedom_of_expression.
684. Internet & Jurisdiction Policy Network. (2018, April). Russian court orders block of Telegram, regulator blocks millions of IP addresses belonging to Google and Amazon. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6952_2018-04.
685. Safi, M. (2018, March 15). Sri Lanka accuses Facebook over hate speech after deadly riots. *The Guardian*. Retrieved from https://www.theguardian.com/world/2018/mar/14/facebook-accused-by-sri-lanka-of-failing-to-control-hate-speech.
686. Internet & Jurisdiction Policy Network. (2018, March). Sri Lanka temporarily blocks access to Facebook for not doing enough in combatting hate speech on their platforms. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6885_2018-03.
687. Internet & Jurisdiction Policy Network. (2019, April). Sri Lanka blocks access to social media in wake of terrorist attacks. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoic3JpIGxhbmthIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==.
688. Silviana, C. (2017, November 8). Indonesia plans automated system to flag contentious Internet material. *Reuters*. Retrieved from https://www.reuters.com/article/us-indonesia-internet/indonesia-plans-automated-system-to-flag-contentious-internet-material-idUSKBN1D815Z?feedType=RSS&feedName=technologyNews.
689. Internet & Jurisdiction Policy Network. (2017, November). Indonesia plans to launch automated flag system to better detect pornography and extremist content online. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6556_2017-11.
690. Internet & Jurisdiction Policy Network. (2019, May). Indonesia restricts access to social media in response to riots. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kb25lc2lhIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==.
691. Mamabolo, M. (2017, September 6). Reports of Togo internet shutdown as anti-govt protests intensify. *IT Web Africa*. Retrieved from http://www.itwebafrica.com/networks/890-togo/240006-reports-of-togo-internet-shutdown-as-anti-govt-protests-intensify?utm_content=bufferf190a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.
692. Internet & Jurisdiction Policy Network. (2017, September). Togo shuts down WhatsApp and slows down internet access as anti-government protests intensify. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6279_2017-09.
693. Internet & Jurisdiction Policy Network. (2017, May). Thailand: Facebook complies with requests to remove content deemed illegal. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-5928_2017-05.
694. Leesa-Nguansuk, S. & Tortermvasana, K. (2017, May 9). Facebook to block local content. *Bangkok Post*. Retrieved from http://www.bangkokpost.com/news/politics/1246010/facebook-to-block-local-content.
695. Gumrukcu, T. (2017, May 5). Turkish court rejects Wikipedia's appeal over website's blocking: Anadolu. *Reuters*. Retrieved from http://www.reuters.com/article/us-turkey-security-internet-wikipedia-idUSKBN18117M.

speech was a fundamental right, it can be limited in cases where there is a 'necessity for regulation.'[696] Following this judicial decision, Wikipedia announced on **May 9** that it had applied to the Turkish constitutional court following the rejection of its appeal.[697] The ban continued and in May 2019 Wikimedia petitioned the European Court of Human Rights to overturn the 2 year ban.[698]

On some occasions, the reasons for blocking a platform at a particular time are not entirely transparent. For example, on November 25, 2017, Twitter stated that the Pakistani government had taken action to block its service, as well as other social media services.[699] The reasoning behind the block was unclear, although, some news outlets have linked it to Islamist protests in Islamabad.[700]

Similarly, on September 25, 2017, text messages sent through WhatsApp were blocked in China, following partial blocks of images and videos in July 2017.[701] While the reasons for the blocking were unclear, news outlets have noted that the decision came ahead of the 19th National Congress of the Chinese Communist Party, a major political event that began on October 18, 2017.[702] There are also variations in procedural steps required before a service may be blocked or shut down. For example, on June 14, 2018, the Belarusian National Assembly amended the country's media law, introducing a requirement for authors of all online posts and comments to identify and register themselves. The government will be able to block social media platforms without the need for a court order. Media platforms must also register with the Information Registry; unregistered media outlets will not enjoy protections granted to the press.

4.2.6

Internet shutdowns

In some extreme cases, governments have opted to shut down internet access entirely within specific countries. Even if they are temporary, such internet shutdowns are fundamentally opposite to the idea of a global internet. After all, internet shutdowns affect not only the people in the country where the shutdown takes place; they also affect anyone outside seeking to communicate with persons or facilities in that country. Furthermore, if a foreign business has invested in the market in question, an internet shutdown may have devastating effects. This is especially true if the foreign business has decided to locate its data in that country, either voluntarily or involuntarily. In the light of this, internet shutdowns are an obvious obstacle to attracting foreign business and investment.

Examples of internet shutdowns are plentiful. In January 2019, the internet was shut down for a time in Zimbabwe,[703] but was restored following a court order finding that Zimbabwe's government exceeded its mandate in ordering an internet blackout during the civilian protests.[704] Similarly, following the general election on December 30, 2018, it was reported that internet access had been restricted in the Democratic Republic of Congo (DRC).[705] A spokesperson for the DRC presidency indicated that internet access, as well as SMS services,

---

696. Gumrukcu, T. (2017, May 5). Turkish court rejects Wikipedia's appeal over website's blocking: Anadolu. *Reuters*. Retrieved from http://www.reuters.com/article/us-turkey-security-internet-wikipedia-idUSKBN18117M.

697. Internet & Jurisdiction Policy Network. (2017, May). Turkey: Wikipedia appeals blocking order in constitutional court. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-5926_2017-05.

698. Internet & Jurisdiction Policy Network. (2019, May). Wikimedia petitions European Court of Human Rights to overturn two year block on Wikipedia in Turkey. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxljoidHVya2V5liwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==.

699. Twitter Public Policy. (2017, November 25). *Pakistani action to block Twitter*. Retrieved from https://twitter.com/policy/status/934471989963689984.

700. Internet & Jurisdiction Policy Network. (2017, November). Twitter announces that it is being blocked by the Pakistani government. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6563_2017-11.

701. Bradsher, K. (2017, September 25). China blocks WhatsApp, broadening online censorship. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html.

702. Internet & Jurisdiction Policy Network. (2017, September). China blocks WhatsApp messaging app. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6277_2017-09.

703. Taye, B. (2019, January 15). Zimbabwe orders a three-day, country-wide internet shutdown. *Access Now*. Retrieved from https://www.accessnow.org/zimbabwe-orders-a-three-day-country-wide-internet-shutdown/.

704. Dzirutwe, M. (2019, January 21). Zimbabwe court says internet shutdown illegal as more civilians detained. *Reuters*. Retrieved from https://www.reuters.com/article/us-zimbabwe-politics/zimbabwe-court-says-internet-shutdown-during-protests-was-illegal-idUSKCN1PF11M.

705. The Guardian. (2019, January 6). *DRC officials postpone presidential election results*. Retrieved from https://www.theguardian.com/world/2019/jan/06/drc-officials-postpone-presidential-election-results.

had been cut after "fictitious results" started appearing.[706]

On December 12, 2017, the Ethiopian government partially blocked access to the internet as student protests grew violent in the Oromia region.[707] Ethiopia has repeatedly restricted access to the internet in recent years, and only one ISP, which is state-owned, currently operates in the country.[708] The end of 2017 also saw a lengthy period of restrictions on internet access in the Anglophone regions of Cameroon.[709] The block was enacted on October 1, 2017, as protests mounted in the Anglophone regions over a perceived failure to uphold the rights of the English-speaking minority. An earlier block the same year was lifted after more than three months, having lasted from January to April 2017.[710] Other recent examples in 2019 of internet shutdowns as a way to crack down on protests and prevent the spread of information include the Indian government's shut down of internet access in Kashmir,[711] the blocking of access by the Algerian government[712] and also by the ruling Sudan military in response to peaceful protests.[713] Benin also experienced an internet shutdown on April 28, 2019 on the day of the legislative elections.[714]

Despite the prevalence of internet shutdowns, there is a widespread recognition that internet shutdowns have a serious negative impact. For example, on June 2, 2017, the African Organisations for Internet Governance (AF*), which includes AFRINIC and other African internet organizations, released a statement criticizing the increasing number of internet shutdowns ordered by Government in Africa, and drawing attention to their negative effects.[715] The statement also criticized a policy, proposed by AFRINIC in April, to restrict access to new IP addresses for governments that engage in internet shutdowns, which AFRINIC formally recanted during the 5th African Internet Summit.[716]

Similarly, the UN Human Rights Council has repeatedly emphasized that it "[c]ondemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures"[717]

Survey recipients highlighted initiatives that are seeking to better inform the impacts of internet shutdowns, including the Cost of Shutdown Tool developed by the Internet Society and Netblocks which is a freely accessible online tool to measure the economic cost of internet shutdowns.[718] Access Now also published its #keepiton Report in 2018 which shows recent trends in internet shutdowns and highlights that they are on the rise.[719]

---

706. Internet & Jurisdiction Policy Network. (2018, December). Democratic Republic of Congo: Internet access restricted following general election. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7739_2018-12.

707. Rahman Alfa Shaban, A. (2017, December 12). Ethiopia restricts internet access amidst new protests. *Africa News*. Retrieved from http://www.africanews.com/2017/12/12/ethiopia-restricts-internet-access-amidst-new-protests/.

708. Internet & Jurisdiction Policy Network. (2017, December). Ethiopia restricts internet access as student protests grow violent. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6627_2017-12.

709. Rahman Alfa Shaban, A. (2017, November 27). Internet restriction in Cameroon's Anglophone region hitting 60-day mark. *Africa News*. Retrieved from http://www.africanews.com/2017/11/27/internet-restriction-in-cameroon-s-anglophone-region-hitting-60-day-mark/.

710. Internet & Jurisdiction Policy Network. (2017, November). Internet access restriction in Cameroon's Anglophone regions reaches 60-day mark. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6565_2017-11.

711. Internet & Jurisdiction Policy Network. (2019, August). India shuts down internet access in Kashmir. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kaWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9.

712. Internet & Jurisdiction Policy Network. (2019, March). Algeria blocks access to the internet in order to crackdown on protests. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiYWxnZXJpYSIsImZyb20iOiIyMDE5LTAxIiwidG8iOiIyMDE5LTA4In0=.

713. Internet & Jurisdiction Policy Network. (2019, July). Partial restoration of internet access in Sudan. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoic3VkYW4iLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9.

714. Amnesty International. (2019, April 28). *Benin: Internet shutdown on election day is a blunt attack on freedom of expression*. Retrieved from https://www.amnesty.org/en/latest/news/2019/04/benin-internet-shutdown-on-election-day-is-a-blunt-attack/.

715. AFRINIC. (2017, June 2). *Common statement by AF* on internet shutdowns in Africa*. Retrieved from https://www.afrinic.net/en/library/news/2141-common-statement-by-af-on-internet-shutdowns-in-africa.

716. Internet & Jurisdiction Policy Network. (2017, June). African internet organizations criticize government shutdowns in joint statement. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6101_2017-06.

717. United Nations, General Assembly. *Human Rights Council: Resolution: Promotion and protection of all human rights, civil, political economical, social and cultural rights, including the right to development*. A/HRC/38/L.10 (2018) p. 3.

718. *Cost of Shutdown Tool*. Retrieved from http://netblocks.org/projects/cost.

719. AccessNow. #KeepItOn. Retrieved from https://www.accessnow.org/keepiton/.

4.2.7

Mandatory data localization

As seen in the Chapter outlining major topical trends (Chapter 3), forced data localization requirements are becoming a widely adopted approach – and, it is argued, a solution – to some of the cross-border legal challenges on the internet. This issue is separate from that of data location as a jurisdictional connecting factor. Nevertheless, it may be interesting to observe how more states attach significance to data location for practical enforcement reasons, while its significance as a jurisdictional connecting factor is almost eradicated.

Examples of mandatory data localization laws are plentiful. For example, on September 10, 2018, it was reported[720] that Google had agreed to comply with data localization requirements set by the Reserve Bank of India (RBI), the country's central bank. The RBI set a deadline of October 15, 2018 for all payment system operators to store the financial data of Indians within the country's territory.[721] While recent amendments have softened the requirements, also India's proposed personal data protection bill incorporated mandatory data localization requirements.[722] This is merely one example of a clear trend. One of the most well-known examples is found in China's Cybersecurity Law which stipulates that sensitive data must be stored domestically.[723] Another example of data localization requirements is Indonesia's Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions ("GR 82") and despite a 5 year transition period operators have sought leniency and more clarification from government on the requirements. The government is reportedly working on a draft amendment to the law.[724]

Data localization – part of the problem, or part of the solution?

When asked whether the increasing number of laws requiring data localization is part of the problem or part of the solution, 47% of surveyed experts indicated that this trend is part of the problem. 31% stated that it is both part of the problem, and part of the solution, while 9.5% took the view that this trend is neither part of the problem, nor part of the solution. Only 12.5% saw the trend as part of the solution.

There were clear sectoral and regional differences among surveyed experts' attitudes toward data localization laws. While the regional sample admittedly is too small to constitute the basis of conclusions, on its own, there is anecdotal evidence – including discussions at recent conferences – supporting the conclusion that data localization is more readily viewed as a solution among Asian countries than elsewhere.

Perhaps it is unsurprising that countries – including countries in Asia – who feel subjected to a form of digital colonization by the countries in which major internet companies are based, would tend to have a more favorable view of data localization. To put it another way, the countries that are primarily receivers of internet services may – correctly or incorrectly – perceive data localization as a tool for power equalization.

> "the countries that are primarily receivers of internet services may [...] perceive data localization as a tool for power equalization."

In their comments, several surveyed experts expressed the view that data localization requirements represent a blunt, dated and inadequate approach to the problem, and that it reflects a failure to resolve legal questions. One respondent pointed to data localization laws as a sign of mistrust in other legal systems; another emphasized that such laws should be partly understood as a response to the current state of affairs, as states' ability to enforce their laws is being undermined. One interviewed expert pointed to concerns about how data being stored outside the jurisdiction of a state will impact that state's sovereignty.

Others raised concerns that forced data localization lacks scalability as an approach, and noted that data localization requirements do not change

---

720. Gupta, K. (2018, September 10). Google agrees to comply with RBI's data localization norms. *Live Mint*. Retrieved from https://www.livemint.com/Companies/xEAFZGZ9kOaMz6R4HIgwXK/Google-ready-to-comply-with-RBI-norms-for-payment-services.html.

721. Internet & Jurisdiction Policy Network. (2018, September). Google agrees to India's central bank's data localization requirements. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7463_2018-09.

722. Singh Mankotia, A. (2019, July 24). Changes likely in proposed data privacy rules: Only critical data may need to be housed in India. *The Economic Times*. Retrieved from https://economictimes.indiatimes.com/tech/internet/changes-likely-in-proposed-data-privacy-rules-only-critical-data-may-need-to-be-housed-in-india/articleshow/70355298.cms?from=mdr.

723. KPMG. (2017, February). *Overview of China's Cybersecurity Law*. Retrieved from https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

724. Innis, M. & Wiyoso, A. (2018, July). General data localization requirements in Indonesia. *Baker McKenzie*. Retrieved from https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al_generaldatalocalizationrequirements_july2018.pdf?la=en.

who is responsible for the data.

Like the surveyed experts, interviewed experts pointed to several weaknesses and risks associated with forced data localization. When imposed widely, forced data localization is very costly for companies to comply with. This, interviewed experts observed, risks entrenching the position and power of the small number of already established companies that can afford, and have the legal and technical expertise, to comply with multiple forced data localization requirements. This, they added, will stifle innovation. Another interviewed expert noted another aspect of the cost factor: the degree to which businesses outside the country will decide to comply with data localization requirements will depend on their desire to economically engage in that country.

One interviewed expert noted that data localization requirements may provide some performance increases. But the same expert also pointed to the risk that, when imposed by small countries, such requirements may simply result in businesses opting not to engage in their markets, resulting in a lack of access to service options and a potential lowering of performance.

Interviewed experts also noted that forced data localization requirements by oppressive regimes may pose risks to rights. For example, in an interview published on April 18, 2018, the head of Russian communications regulator *Roskomnadzor* stated that Facebook could be blocked if the platform does not show compliance with Russian data localization requirements.[725] *Roskomnadzor* had already warned the platform that it would be blocked unless it complied with its data localization rules in September 2017.[726] In November 2016, LinkedIn was blocked for refusing to comply with the rules.[727] In April 2019, a Russian court fined Facebook and Twitter for not providing information in compliance with the data localization requirements.[728]

Finally, despite all the attention directed at forced data localization requirements, it is worth noting that data localization occurs on a voluntary basis, as well. In fact, given that data always needs to be stored at some physical location, voluntary data localization choices are exceedingly common and are affected by a wide range of factors.

4.2.8

Artificial Intelligence

Artificial intelligence (AI), while not a new phenomenon, has recently captured the attention of all the Internet & Jurisdiction Policy Network's stakeholder groups. Indeed, arguably no other topic discussed in this section of the Report transcends, and indeed unifies, the three areas of expression, economy and security, in the way AI does. Consequently, the impact of AI and related technical developments such as machine learning, algorithmic decision-making and other forms of automated data processing are relevant for several parts of this Report.

Any discussion of the increasing responsibility bestowed on private operators (through laws making internet platforms the gatekeepers of content) must account for the potential of AI as a content moderator – one that can be implemented on multiple levels and by multiple stakeholders.[729] Several interviewed experts predicted that policy makers will call for platforms to implement AI to detect and remove unlawful content, at least in relation to some categories of illegality. As this happens, issues such as algorithmic biases, over-blocking, lack of transparency, lack of remedies and liability concerns have already arisen, and will only grow in intensity.[730]

AI stands to transform most, if not all, aspects of society. It plays an increasingly large role in the operation of our mobile phones and home computer systems, and in the way information is accessed and shared; AI affects the types of jobs available and how employees work in the jobs that remain; it improves health diagnostics; and it carries huge economic implications:

> "PwC has estimated that AI could contribute up to $15.7 trillion to the global economy in 2030, more than the current output of China and India combined. Of this, $6.6 trillion likely will come from increased productivity due to automation of tasks and roles

---

725. Sputnik International. (2018, April 18). *Russia's watchdog may block Facebook if network fails to comply with laws*. Retrieved from https://sputniknews.com/russia/201804181063669626-russia-watchdog-may-block-facebook/.

726. Internet & Jurisdiction Policy Network. (2018, April). Russian regulator says Facebook will be blocked unless it complies with data localization requirements. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6961_2018-04.

727. Internet & Jurisdiction Policy Network. (2016, November). Russia blocks LinkedIn for non-compliance with data localization rules. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-4192_2016-11.

728. Moscow Times. (2019, April 12). Russia fines Facebook for failing to provide information on user data. Retrieved from https://www.themoscowtimes.com/2019/04/12/russia-fines-facebook-for-failing-to-provide-information-on-user-data-a65225.

729. MacCarthy, M. (2018, October 26). AI-driven content moderation can never be perfect. *CIO*. Retrieved from https://www.cio.com/article/3316562/artificial-intelligence/artificial-intelligence-driven-content-moderation-can-never-be-perfect.html.

730. See e.g.: Hutt, J.J. (2018, April 26). Why YouTube shouldn't over-rely on artificial intelligence to police Its platform. *ACLU*. Retrieved from https://www.aclu.org/blog/privacy-technology/internet-privacy/why-youtube-shouldnt-over-rely-artificial-intelligence.

and $9.1 trillion likely will come from product enhancements that stimulate consumer demand."[731]

AI may transform the national security arena, as well. As recently noted: "Three of the world's biggest players, US, Russia, and China, are entrenched in non-kinetic battle to out-pace the other in AI development and implementation."[732]

AI also poses risks in relation to the creation and distribution of undesirable online content such as hate speech, bullying and deep fakes. There are concerns that AI may be contribute to the 'junkification of the internet' in a manner that undermines the internet's value.

Considering the above, there can be no doubt that AI will impact many, if not most, of the issues discussed in this Report, and needs to be carefully monitored over the coming years.

> "arguably no other topic discussed in this section of the Report transcends, and indeed unifies, the three areas of expression, economy and security in the way AI does."

Some recent key developments and publications on AI include the following:

In **September 2019**, the **World Economic Forum** published its White Paper titled AI Government Procurement Guidelines.[733]

At the **G20** Ministerial Meeting on Trade and Digital Economy in **June 2019** in Tsubuka, Japan, the G20 Trade and Digital Economy Ministers endorsed the G20 AI Principles focusing on a human-centred approach to AI.[734]

The **OECD** adopted its Principles on Artificial Intelligence in **May 2019**.[735]

In **January 2019**, **Singapore**'s Personal Data Protection Commission published its Model AI Governance Framework.[736] Consultation has taken place during the first half of 2019.[737] And in **November 2018**, The Monetary Authority of Singapore (MAS) released a set of principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence (AI) and data analytics in finance.[738]

In **2018,** 32 **UN** bodies/agencies and the **ITU** published a report titled United Nations Activities on Artificial Intelligence (AI), outlining how various UN agencies use AI technologies to achieve their objectives.[739]

---

731. PwC. (2018). *Top policy trends of 2018*. Retrieved from https://www.pwc.com/us/en/risk-regulatory-consulting/assets/top-policy-trends-2018.pdf, p. 13.
732. Garcia, E. (2018, April 19). The artificial intelligence race: US, China and Russia. *Modern Diplomacy*. Retrieved from https://moderndiplomacy.eu/2018/04/19/the-artificial-intelligence-race-u-s-china-and-russia/.
733. World Economic Forum. *AI Government Procurement Guidelines*. Retrieved from https://www.weforum.org/whitepapers/ai-government-procurement-guidelines.
734. G20. (2019, June). *G20 AI Principles*. Retrieved from http://k1.caict.ac.cn/yjts/qqzkgz/zksl/201906/P020190610727837364163.pdf.
735. OECD. *OECD Principles on AI*. Retrieved from http://www.oecd.org/going-digital/ai/principles/.
736. Personal Data Protection Commission Singapore. *Proposed Model AI Governance Framework*. Retrieved from https://www.pdpc.gov.sg/Resources/Model-AI-Gov.
737. Personal Data Protection Commission Singapore. *Proposed Model AI Governance Framework*. Retrieved from https://www.pdpc.gov.sg/Resources/Model-AI-Gov.
738. Monetary Authority of Singapore. (2018, November). *Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector*. Retrieved from https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf.
739. United Nations and International Telecommunication Union. (2018). *United Nations activities on artificial intelligence*. Retrieved from https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2018-1-PDF-E.pdf.

In **December 2018**, the **European Commission**'s High-Level Expert Group on Artificial Intelligence published its Draft Ethics Guidelines for Trustworthy AI.[740] Following further consultations, the revised Guidelines were published in **2019**.[741] In 2019, the EU also launched the European AI Alliance, an open discussion platform.[742]

In **December 2018**, the **Council of Europe** adopted a text setting out ethical principles relating to the use of artificial intelligence in judicial systems.[743] The **Council of Europe** has also – on 11 September 2019 – set up an Ad Hoc Committee on Artificial Intelligence,[744] and have published numerous reports and declarations over recent years such as:

- Unboxing Artificial Intelligence: 10 steps to protect Human Rights[745] of **May 2019**.
- Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes,[746] of **February 2019**.
- Draft Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes,[747] of **November 2018**.
- Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems,[748] of **November 2018**.
- A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework,[749] of **November 2018**.
- Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications,[750] of **December 2017**.

UNESCO has arranged events such as its Forum on Artificial Intelligence in Africa in **December 2018**.[751]

In **November 2018**, the **German** Federal Government's Artificial Intelligence (AI) strategy was published.[752]

---

740. European Commission's High-Level Expert Group on Artificial Intelligence. (2018, December 18). *Draft ethics guidelines for trustworthy AI.* Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56433.
741. European Commission. (2019, April 8). *Ethics guidelines for trustworthy AI.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
742. European Commission. *The European AI Alliance.* Retrieved from https://ec.europa.eu/digital-single-market/en/european-ai-alliance.
743. Council of Europe. (2018, December 4). *Council of Europe adopts first European Ethical Charter on the use of artificial intelligence in judicial systems.* Retrieved from https://www.coe.int/en/web/artificial-intelligence/-/council-of-europe-adopts-first-european-ethical-charter-on-the-use-of-artificial-intelligence-in-judicial-systems.
744. Council of Europe. (2019, September 11). *The Council of Europe established an ad hoc committee on Artificial Intelligence – CAHAI.* Retrieved from https://www.coe.int/en/web/artificial-intelligence/-/the-council-of-europe-established-an-ad-hoc-committee-on-artificial-intelligence-cahai.
745. Council of Europe. (2019, May). *Unboxing artificial intelligence: 10 steps to protect human rights.* Retrieved from https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.
746. Council of Europe (2019, February 14). *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes.* [Press Release]. Strasbourg. Retrieved from https://www.coe.int/en/web/data-protection/-/declaration-by-the-committee-of-ministers-on-the-manipulative-capabilities-of-algorithmic-processes.
747. Council of Europe. (2018, November 16). *Draft Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes* MSI-AUT(2018)07. Retrieved from https://rm.coe.int/draft-declaration-on-the-manipulative-capabilities-of-algorithmic-proc/16808ef257.
748. Council of Europe. (2018, November 12). *Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems* MSI-AUT(2018)06. Retrieved from https://rm.coe.int/draft-recommendation-on-human-rights-impacts-of-algorithmic-systems/16808ef256.
749. Council of Europe. (2018, November 9). *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework* MSI-AUT(2018)05. Retrieved from https://rm.coe.int/draft-study-of-the-implications-of-advanced-digital-technologies-inclu/16808ef255.
750. Council of Europe. (2017, December). *Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications* DGI(2017)12. Retrieved from https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10.
751. UNESCO. (2019, September 9). *UNESCO engages technology and policy experts for human centered AI in Africa.* Retrieved from https://en.unesco.org/news/unesco-engages-technology-and-policy-experts-human-centered-ai-africa.
752. Die Bundesregierung. *Nationale KI strategie.* Retrieved from https://www.ki-strategie-deutschland.de/home.html. English language version of the strategy document is here: https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf.

Making specific reference to agriculture, healthcare, public services and financial services, a **November 2018** white paper by Access Partnership and the University of Pretoria noted: "The rapidly developing set of artificial intelligence (AI) technologies has the potential to solve some of the most pressing challenges that impact **Sub-Saharan Africa** and drive growth and development in core sectors".[753] However, in its **November 2018** report Coming to Life: Artificial Intelligence in Africa,[754] the Atlantic Council notes that:

- "Unfortunately, except in a handful of countries—namely **Kenya, South Africa, Nigeria, Ghana, and Ethiopia**—the application of AI is a chimera, not a reality. The critical factors necessary for the technology to take hold are woefully absent across most of the continent, and many African countries remain incapable of requisite reforms in the areas of data collection and data privacy, infrastructure, education, and governance. Without those reforms, there is little chance that most African nations will be able to exploit AI technologies to advance sustainable development and inclusive growth. The specter of automation threatens to leave these countries behind."[755]

In **November 2018**, **Access Now** published its report on Human Rights in the Age of Artificial Intelligence.[756]

In **September 2018**, the World Wide Web Foundation published its report titled Algorithms and Artificial Intelligence in **Latin America**.[757]

In **September 2018**, the Subcommittee on Information Technology Committee on Oversight and Government Reform of the **US** House of Representatives issued a white paper titled Rise of the Machines: Artificial Intelligence and its Growing Impact on U.S. Policy.[758]

In **June 2018**, the National Institution for Transforming **India** (NITI Aayog) released a white paper on the development of a comprehensive national AI strategy.[759]

Amnesty International and Access Now launched the Toronto Declaration: Protecting the Rights to Equality and Non-discrimination in Machine Learning Systems at RightsCon in Toronto, **Canada** in **May 2018**.[760]

In **April 2018**, **ARTICLE 19** and **Privacy International** published a report titled Privacy and Freedom of Expression in the Age of Artificial Intelligence.[761] ARTICLE 19 published a further report in **April 2019** titled Governance with Teeth: How Human Rights can Strengthen FAT and Ethics Initiatives on Artificial Intelligence.[762]

---

753. Access Partnership and University of Pretoria. (2018, November). *Artificial intelligence for Africa: An opportunity for growth, development and democratisation*. Retrieved from https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf, p. 3.
754. Gadzala, A. (2018, November). Coming to life: Artificial intelligence in Africa. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf.
755. Gadzala, A. (2018, November). Coming to life: Artificial intelligence in Africa. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf, p. 1.
756. Access Now. (2018, November). *Human rights in the age of artificial intelligence*. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.
757. World Wide Web Foundation. (2018, September). *Algorithms and artificial intelligence in Latin America*. Retrieved from http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Screen_AW.pdf.
758. Subcommittee on Information Technology, Committee on Oversight and Government Reform of the U.S. House of Representatives. (2018, September). *Rise of the machines: Artificial intelligence and its growing impact on U.S. Policy*. Retrieved from https://oversight.house.gov/wp-content/uploads/2018/09/AI-White-Paper-.pdf.
759. National Institution for Transforming India. (2018, June). *Discussion paper: National strategy for artificial intelligence*. Retrieved from http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
760. Amnesty International and Access Now. (2018, May). *Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems*. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf.
761. ARTICLE19 & Privacy International. (2018, April). *Privacy and freedom ofeExpression In the age of artificial intelligence*. Retrieved from https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf.
762. ARTICLE19. (2019, April). *Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence*. Retrieved from https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf.

It has been noted that "**China** has the capability and opportunity to lead international collaboration in the development and governance of AI, ensuring that this breakthrough technology will positively contribute to the general welfare of all humanity".[763] In **January 2018**, the China Electronics Standardization Institute published its Artificial Intelligence Standardization Whitepaper, "which summarizes current developments in AI technology, standardization processes in other countries, China's AI standardization framework and China's plan for developing AI capabilities going forward."[764]

In **2017**, the Group of Seven (G7) – comprising of **Canada, France, Germany, Italy, Japan, the UK and the US** – issued its Innovation Ministers' Statement on Artificial Intelligence.[765]

A **2017** McKinsey Global Institute report observed that: "**China** and the **United States** are currently the world leaders in AI development. In 2015 alone, they accounted for nearly 10,000 papers on AI published in academic journals, while the **United Kingdom, India, Germany, and Japan** combined to produce only about half as many scholarly research articles."[766]

In **October 2017**, the **United Arab Emirates** released an AI strategy.[767]

A topic that so far has gained only limited attention, is the extent to which AI may help overcome some of the challenges with which this Report is concerned. Yet, this topic has the potential to become increasingly important. Indeed, AI may potentially assist with anything from helping individual and companies navigate the complex regulatory landscape online, to being utilized by courts either to inform the court, or even to directly or indirectly decide disputes.[768]

---

763. McKinsey Global Institute. (2017, April). *Artificial intelligence: Implications for China.* Retrieved from https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx, p 1.
764. Luo, Y., Kaja, A. & Karch, T.J. (2018, July 16). China's framework of AI standards moves ahead. *The National Law Review.* Retrieved from https://www.natlawreview.com/article/china-s-framework-ai-standards-moves-ahead.
765. G7. (2018). *Annex B: G7 Innovation Ministers' Statement on Artificial Intelligence.* Retrieved from https://g7.gc.ca/en/g7-presidency/themes/preparing-jobs-future/g7-ministerial-meeting/chairs-summary/annex-b/.
766. McKinsey Global Institute. (2017, April). *Artificial intelligence: Implications for China.* Retrieved from https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx, p. 4.
767. United Arab Emirates. (2017, October). *UAE Artificial intelligence strategy.* Retrieved from http://www.uaeai.ae/en/.
768. Svantesson. D, J. B. (2019, August 4). Vision for the future of private international law and the Internet – Can artificial intelligence succeed where humans have failed?. *Harvard International Law Journal Blog.* Retrieved from https://harvardilj.org/2019/08/a-vision-for-the-future-of-private-international-law-and-the-internet-can-artificial-intelligence-succeed-where-humans-have-failed/.

05

RELEVANT CONCEPT CLUSTERS 101

EXPRESSION

SECURITY

ECONOMY

As noted (Chapter 1.5), and as observed by interviewed and surveyed experts, progress on the cross-border legal challenges faced on the internet has been hindered, in part, by the insufficiency of the framework and concepts we use to address these challenges. The entire field suffers from a pronounced 'artificial regulatory challenge'.

The current conceptual complexity in the field of cross-border legal challenges faced on the internet prevents informed participation for many stakeholders, and frequently results in misunderstanding, miscommunication and avoidable disagreement.

There are numerous concepts that must be understood and agreed upon in order to foster a productive discussion of the issue. Complicating matters further is the fact that these concepts are often only properly understood when viewed in relation to other related concepts.

This Chapter highlights the variety of relevant 'concept clusters', with the aim to both discuss a selection of concepts and illustrate how they relate to each other. Some key concepts – such as the concept of 'jurisdiction' – must be viewed in relation to several other concepts and are thus discussed as part of several clusters.

5.1

Public international law, private international law (or conflict of laws)

The discipline of **public international law** is traditionally described as a legal order that structures interactions between states. There is recent recognition, however, that the discipline also encompasses other international law subjects, and relationships between individuals and states.

In contrast, **private international law** (or **conflict of laws,** as the discipline often is referred to in Common Law countries),[769] is the part of domestic law that governs relations (across different legal jurisdictions) between natural persons, companies, corporations and other legal entities.

This distinction, while still prevalent, has been subject to criticism for a long time, and is arguably becoming more difficult to maintain:

> "From a functional point of view, the distinction between public and private international law would appear to be at best artificial, as both public and private international law ultimately deal with the myth and practice of responding to claims for the allocation of the good as well as the undesirable things in the world social processes. [...] [P]ublic and private international law are in reality complementary and indispensable components of a larger and more inclusive conception of world public order."[770]

An area like data privacy law, for example, seems to fit partly in public international law and partly in private international law. Furthermore, the

769. For a detailed discussion of private international law as applied to the internet see e.g.: Svantesson, D. (2016) *Private International Law and the Internet* (3rd ed.). Alphen aan den Rijn, The Netherlands: Kluwer Law International.

770. Nagan, W.P. (1981-82). Conflicts theory in conflict: A systematic appraisal of traditional and contemporary theories. *Journal of International and Comparative* Law, 3(3), 343-546, 361.

cross-border legal challenges faced on the internet are much the same whether they arise within public international law (as traditionally defined) or in private international law; both public and private international law are aimed at "allocating among states of the world the competence to make and apply law to the transnational events that affect them".[771] Finally, it should be noted that if a remedy granted under private law is ignored, public law may impose sanctions. Therefore, private law matters that initially raise jurisdictional issues under private international law may later raise jurisdictional issues under public international law, as well.

Against this background, it is fruitful to approach internet jurisdiction as a homogenous field of study.

5.2

Sovereignty, jurisdiction, territory and human rights

The term **jurisdiction** has more than one meaning.[772] Here, it is used to signify the power to hear a matter, e.g., where a court has jurisdiction over a given dispute.

The concept of **sovereignty**[773] is typically described as involving supreme authority within a territory. There is, therefore, a clear link between sovereignty, jurisdiction and **territory**, though this link is often misunderstood.

While territoriality traditionally plays an important role in relation to jurisdiction, the concept of sovereignty does not always demand that jurisdiction be based on territoriality, alone. To see that this is so, one need only consider established international law concepts such as the nationality principle that authorizes jurisdictional claims based on the nationality of the person in question.

Moreover, while international law may demand that there be only one sovereign over a given territory, it is clear that an individual or matter may be subject to more than one sovereign power. Sovereignty should not necessarily be understood to signify exclusiveness in all settings; sovereignty-based exclusiveness, in relation to persons and matters, is a poor fit with the interconnected world.[774]

There is an ongoing debate about how the concept of sovereignty applies online. This debate gets to the core of the concept of sovereignty; some have raised questions as to whether sovereignty is itself a binding rule of international law, or rather a principle of international law that guides state interactions but does not dictate results under international law.[775] This has far-reaching implications in general but also for claims of so-called 'data sovereignty' and 'information sovereignty' – terms often used without any clear consensus on their precise meanings.

This takes us to the long-standing tension between sovereignty on the one hand, and human rights on the other hand. The relationship, or indeed hierarchy, between sovereignty and human rights is of crucial importance. The traditionally Western view that human rights override sovereignty, necessarily imposes limitations on what states can do. However, for example, under former Soviet international law doctrine, sovereignty took priority over human rights,[776] and under the Soviet concept of 'information sovereignty', "the State has a right to control the dissemination of information within its territory."[777] Such sentiments are increasingly common in relation to the internet, and the tension between sovereignty and human rights remains of central importance.

---

771. McDougal, M. & Jasper, R. (1982). The Foreign Sovereign Immunities Act of 1976: Some suggested amendments. In M. Landwehr (Ed.), *Private investors abroad—Problems and solutions in international business in 1981*. New York, NY: M. Bender, 6.

772. For a detailed discussion of jurisdiction as applied in public international law see e.g.: Ryngaert, C. (2015) *Jurisdiction in International Law* 2nd edn. Oxford, United Kingdom: Oxford University Press. See also: Schmitt, M. (Ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom, Cambridge University Press, 51-78.

773. For one view on the topic of sovereignty as applied online see e.g.: Schmitt, M. (Ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom, Cambridge University Press, 11-29.

774. See further: Polcak, R. & Svantesson, D. (2017). *Information sovereignty – Data privacy, sovereign powers and the rule of law*. Cheltenham, UK: Edward Elgar Publishing, 63-65.

775. See further: Ginsburg, T. (2017). Introduction to symposium on sovereignty, cyberspace, and Tallinn Manual 2.0. *AJIL Unbound*, 111, 205–206; Wright, J. (2018, May 23). *Cyber and international law in the 21st century*. Retrieved from https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

776. Österdahl, I. (1992), *Freedom of Information in Question*. Uppsala, Sweden: Iustus Förlag AB, 136-137.

777. Österdahl, I. (1992), *Freedom of Information in Question*. Uppsala, Sweden: Iustus Förlag AB, 137.

5.3

Territorial, and extraterritorial, jurisdictional claims

A distinction is often drawn between territorial and extraterritorial jurisdictional claims. Unfortunately, the implications of extraterritorial jurisdictional claims are often overstated with regard to international law. In fact, **the territorial/extraterritorial dichotomy** is sometimes misused as shorthand for distinguishing between legitimate and illegitimate claims of jurisdiction. However, just as there may be perfectly legitimate extraterritorial claims of jurisdiction under international law, there may be questionable territoriality based claims of jurisdiction, as well.

In addition, under international law there is no clear consensus on how to define a jurisdictional claim as extraterritorial. As illustrated in the 2018 *Microsoft Warrant* case,[778] for example, even legal systems that include an express presumption against extraterritoriality lack a clear definition of extraterritoriality in the online context. This further undermines the usefulness of the territorial/extraterritorial dichotomy as a tool for addressing cross-border legal challenges on the Internet.

5.4

Due diligence, duty of non-intervention and comity

The concept of comity is found in both international law and the laws of various states. It lacks a uniform definition and may not necessarily carry the same meaning in the international arena as it does in a state's domestic laws. Nevertheless, **the general idea of comity** is that a state must consider the rights and interests of other states.[779] Thus, in the context of the cross-border legal challenges faced on the internet, the concept of comity is an important reminder that even if a state making a claim of jurisdiction has a strong connection to, and interest in, the matter at hand, it must also consider the rights and interests of other states before deciding to claim jurisdiction.

The **duty of non-intervention** (or 'the principle of non-interference') is a direct consequence of sovereignty; states enjoy sovereignty, and other states must take steps to avoid interfering with that sovereignty.[780] Therefore, like the concept of comity, the duty of non-intervention underscores the necessity of accounting for the rights and interests of other states when making jurisdictional claims.

While discussions of internet jurisdiction typically focus on restrictions on jurisdiction, such as those imposed by the concept of comity and the duty of non-intervention, international law may also mandate claims of jurisdiction in certain circumstances. Under the **due diligence principle** (and the overlapping 'no harm principle'), a state is essentially obliged to ensure that other states' rights and interests are not violated under its jurisdiction.[781]

Together, these three concepts impose an obligation for states to account for the interests of other states in deciding whether to claim jurisdiction over a specific matter or person.

---

778. Wikipedia. *Microsoft Corp. v United States*. Retrieved from https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States.

779. See e.g.: Hilton v Guyot 159 US 113 (1895) 164.

780. See e.g.: Crawford, J. (2012). *Brownlie's principles of public international law* (8th ed.). Oxford, UK: Oxford University Press.

781. See further: Corfu Channel (United Kingdom v Albania) [1949] ICJ Rep 4.

5.5

Legislative jurisdiction, adjudicative jurisdiction, investigative jurisdiction and enforcement jurisdiction

In public international law, jurisdictional claims traditionally fall under the categories of:

1. **legislative (or prescriptive) jurisdiction** – i.e., the power to make its law applicable to the activities, relations or persons;
2. **adjudicative (or judicial) jurisdiction** – i.e., the power to subject persons or things to the process of its courts or administrative tribunals; or
3. **enforcement jurisdiction** – i.e., the power to induce or compel compliance or punish noncompliance with its laws or regulations.

A fourth category – **investigative jurisdiction** – is increasingly recognized, as well.[782] While investigative measures have traditionally been treated as an aspect of enforcement jurisdiction, such measures radically differ from other categories of conduct (such as arrests on foreign soil) that are also classified as claims of enforcement jurisdiction. There is, therefore, little merit in bundling such distinct matters under one heading.

The neat categorization outlined above is something of an illusion. As illustrated by the discussion in and around the seminal *Lotus* case,[783] there is not always agreement on the category to which a given jurisdictional claim belongs.

Furthermore, it is often assumed that the impacts of claims of enforcement jurisdiction are necessarily more severe than the consequences of legislative jurisdiction or adjudicative jurisdiction claims. Yet, this is an oversimplification. Ultimately, the impact of each jurisdictional claim must be assessed regardless of category; and the greater the potential for a jurisdictional claim has to interfere with the sovereignty of another state, the greater the reason to limit the exercise of jurisdiction.

5.6

Jurisdiction, choice of law, declining jurisdiction, recognition and enforcement

Private international law addresses four types of issues.[784] The first is the question of **jurisdiction** – the court's power to hear the dispute. The second is the matter of **choice of law**. Choice of law is an important matter because once a court decides to claim jurisdiction, it may, for a variety of reasons, decide to apply foreign substantive law, and the applicable law will determine the outcome of any dispute.

A court that has determined that it may claim jurisdiction over a given dispute may nevertheless decide not to exercise that jurisdiction. This is known as **the court's power to decline to exercise jurisdiction**. The grounds upon which the court may reach such a conclusion vary considerably across countries. In general, courts in the Common Law tradition have wider discretion (particularly via the doctrine of *forum non conveniens*[785]) in comparison to their Civil Law counterparts, which can typically only decline jurisdiction if an action is already pending in another court (*lis alibi pendens*[786]).

Finally, if a court in one country has decided a substantive dispute, the resulting judgment may need to be **recognized and enforced** in another country.

These four components are intertwined, and best viewed as a system where changes to the rules of one are likely to affect the rules of the others.

---

782. See e.g.: Lawson v Accusearch Inc dba Abika.com [2007] 4 FCR 314 and Weltimmo s.r.o.v. Nemzeti Adatvédelmi és Információszabadság Hatóság (Case C- 230/ 14). See also: Svantesson, D. (2012). Extraterritoriality in the context of data privacy regulation. *Masaryk University Journal of Law and Technology* 7(1) 87-96, 92-93. Retrieved from https://journals.muni.cz/mujlt/article/viewFile/2628/2192.

783. SS 'Lotus' (France v Turkey) (1927) PCIJ Series A, No 10.

784. Svantesson, D. (2016). *Private international law and the internet* (3rd ed.). Alphen aan den Rijn, The Netherlands: Kluwer Law International.

785. Under the doctrine of *forum non conveniens* a court may decline to exercise jurisdiction due to it being 'a clearly inappropriate forum' (under Australian law), or more commonly, due to there being another court that may more appropriately hear a case.

786. *Lis alibi pendens* instructs a court to stay a lawsuit where another lawsuit is pending elsewhere. Thus, the ultimate goal is to avoid contradictory judgments on the same matter.

5.7

Personal jurisdiction, subject matter jurisdiction and scope of jurisdiction

A distinction is often drawn between personal jurisdiction and subject matter jurisdiction. **Personal jurisdiction** relates to a court having jurisdiction over a particular legal or natural person. **Subject matter jurisdiction** relates to whether a court has jurisdiction over the type of dispute in question.

Recent litigation, however, has brought attention to a third type of jurisdictional issue: 'scope of jurisdiction'. **Scope of jurisdiction** relates to the geographical scope of orders rendered by a court that has personal jurisdiction and subject-matter jurisdiction. This issue – which overlaps with the law of remedies – has lately arisen with courts making global blocking, de-referencing or content removal orders.

Considerations as to the appropriate scope of jurisdiction are intrinsically linked to the strength of the relevant claim of personal jurisdiction, as well as to the choice of law. For example, where a court has a relatively weak claim of personal jurisdiction, it may not be in a position to opt for an expansive scope of jurisdiction. A court opting for an expansive scope of jurisdiction may also not be able to apply only its own law, given the impact its judgment will have abroad.

5.8

Technology neutral, functional equivalence, future proofing

Given the speed with which technology develops, laws enacted today risk being outdated even before they come into effect. As a result, laws may fail to: (1) regulate conduct to which they should apply, and/or (2) regulate conduct to which they should not apply.

To address these concerns, law makers have long sought to develop **technology-neutral laws**. Such laws are not anchored in terminology and concepts that are technology-specific and, therefore, are likely to date quickly. Technology-neutral laws are thus better equipped to address the first of the two risks identified above. But one may argue that compared to technology-specific laws, technology-neutral laws are at greater risk of regulating conduct to which they should not apply.

The related idea of **functional equivalent laws** aims to ensure that laws regulate internet conduct in the same way they regulate equivalent offline conduct.

Future proofing laws is a broader concept that, essentially, draws attention to: (1) how potential future developments may impact the application of the law in question, and (2) how the law in question may impact potential future developments.

5.9

Data types

Various data classifications have emerged across different settings, and unfortunately, with little coordination. In the setting of data privacy, a distinction is typically drawn between data that amounts to 'personal data' and data that does not. This distinction is crucial, as data privacy laws ordinarily only regulate personal data. Of the data that qualifies as personal data, some types are viewed as sensitive data, and may be afforded the protection of additional safeguards.

Data classification has also emerged in cases where law enforcement seeks to access privately held data.[787] Here, a distinction is often made between metadata and content data. Metadata is sometimes divided into subcategories: most commonly, 'subscriber information' and 'traffic data'. But it is sometimes divided into three subcategories – 'subscriber data', 'access data', and 'transactional data' – as is the case in the recent EU proposals on this topic.[788]

---

787. For a detailed discussion of this see: Warken. C., van Zwieten, L. & Svantesson, D. (2019). Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence. *International Review of Law, Computers & Technology*.

788. European Commission. (2018, April 17). *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.* COM (2018) 226 final and European Commission, (2018, April 17). *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.* COM (2018) 225 final.

5.10

Delist, deindex, de-reference, delete, block, remove, takedown, stay-down

The terminology of court orders aimed at dealing with unlawful content has exploded in variety in recent years. Several terms are used interchangeably; orders to **delete**, **remove** or **takedown** content, for example, order a party to cease making the content in question available online. In contrast, orders to **delist**, **deindex**, **de-reference** or **block** content are aimed at forcing a party – typically an intermediary, such as a search engine or an internet platform – to make the relevant content unavailable on the platform in question.

Finally, it is worth noting the difference between 'takedown' and '**stay-down**'. The former has already been explained. The latter goes further, requiring the party in question to take steps to prevent the content from re-appearing.[789]

5.11

Registry, registrar, gTLD and ccTLD

The governance of domain name system (DNS) is structured in layers. An organization that manages top-level domain names is known as a domain name **registry**. The role of a registry includes creating domain name extensions, setting the rules for the domain names under that top-level domain, and working with registrars to sell domain names to the public. A **registrar** is an organization – accredited by a domain name registry – that sells domain names to the public.

It is also important to distinguish between **generic top-level domains** (gTLDs) and **country code top-level domains** (ccTLDs). As some interviewed experts emphasized, gTLDs are global in nature, and gTLD registrars are bound by a contractual structure with ICANN. In contrast, ccTLDs are regulated by national laws and procedures.

The same interviewed expert noted that, although approximately 45% of domain names in the world are ccTLDs, most discussions seem focused on gTLDs.

5.12

Internet, World Wide Web

While one sometimes sees the terms internet and World Wide Web (WWW) used as synonyms, such interchangeable usage is incorrect. The **internet** is the technical infrastructure that connects computers around the world and is often described as a network of networks. It is, therefore, possible, in theory, to imagine a content-less internet. But, most references to the internet seem to implicitly incorporate the content available on the internet. Thus, the term 'internet', as most commonly used, has both a physical dimension (the technical infrastructure) and a digital dimension (the content). Both these dimensions create potential jurisdictional connection points.

Communications on the internet are controlled by various protocols. **WWW** uses the Hypertext Transfer Protocol (HTTP). Users may operate software called web browsers to access webpages that may be connected via so-called hyperlinks. WWW is merely one of several communications forms that are built on the internet. Others include, email (based on the Simple Mail Transfer Protocol (SMTP)) and the File Transfer Protocol (FTP), commonly used for transmitting files over the internet.

---

789. Romero-Moreno, F. (2018). 'Notice and staydown' and social media: amending Article 13 of the Proposed Directive on Copyright. *International Review of Law, Computers & Technology*, 1–24.

5.13

B2B, B2C, and C2C

Transactions between two businesses are commonly referred to as **business-to-business (B2B)** transactions. If, for example, a department store purchases a sophisticated computer system from a manufacturer, the two companies engage in a B2B transaction. If, on the other hand, a natural person purchases a book from an online bookstore (outside of her/his professional capacity), a **business-to-consumer (B2C)** transaction takes place.

Both B2B and B2C transactions have occurred online for a relatively long period of time. The third category, **consumer-to-consumer (C2C)** transactions, are comparatively more recent. In a C2C transaction, neither party acts in their professional capacity. A typical example of such a transaction involves a natural person purchasing an object from another natural person through an online trading platform.

5.14

Strong, moderate and weak artificial intelligence

There are numerous definitions of artificial intelligence, and a variety of ways in which to conceptualize different types of AI.

The Council of Europe, for example, defines AI as "a set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. Current developments aim, for instance, to be able to entrust a machine with complex tasks previously delegated to a human."[790]

The Council also notes the distinction between what has been termed 'strong' AI, with the ability to "contextualize very different specialized problems completely independently," and 'weak' to 'moderate' AI, with the ability to "perform extremely well in their field of training."[791] Strong AI is generally beyond the reach of current technologies.

This – the classification of AI as being strong, moderate or weak – is of course only one way in which to categorize AI. Another common approach is to distinguish between different AI technologies, such as machine learning and natural language processing (NLP). Put simply, machine learning involves learning algorithms exposed to training data resulting in software with the ability to make predictions or decisions without being explicitly programmed to perform the task.[792] NLP is "concerned with the interactions between computers and human (natural) languages, in particular how to program computers to process and analyze large amounts of natural language data."[793]

Finally, it should be noted that AI often is discussed in the context of a variety of other 'buzzwords' such as automation and data mining. Both automation and data mining[794] can, but need not be, based on AI.

---

790. Council of Europe, *Glossary*. Retrieved from https://www.coe.int/en/web/artificial-intelligence/glossary.
791. Council of Europe, *Glossary*. Retrieved from https://www.coe.int/en/web/artificial-intelligence/glossary.
792. Wikipedia. *Machine learning*. Retrieved from https://en.wikipedia.org/wiki/Machine_learning.
793. Wikipedia. *Natural language processing*. Retrieved from https://en.wikipedia.org/wiki/Natural_language_processing.
794. For a detailed discussion of the relationship between law and data mining see e.g.: Colonna, L. (2016). *Legal Implications of Data Mining*. Tallinn, Estonia: Tallinna Raamatutrükikoda.


INTERNET &
JURISDICTION
POLICY NETWORK

The Internet & Jurisdiction Policy Network is the multistakeholder organization addressing the tension between the cross-border nature of the internet and national jurisdictions.

Its Secretariat facilitates a global policy process between key stakeholders to enable transnational cooperation and policy coherence. Participants in the Policy Network work together to preserve the cross-border nature of the Internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 300 key entities from different stakeholder groups around the world, including governments, the world's largest Internet companies, the technical community, civil society groups, leading universities and international organizations.