United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

THE STATE OF INTERNATIONAL COOPERATION FOR LAWFUL ACCESS TO DIGITAL EVIDENCE:

RESEARCH PERSPECTIVES

CTED TRENDS REPORT
JANUARY 2022

****

This report has been made possible through funding provided by Germany. It has been prepared for informational purposes only. Its content does not necessarily represent the views or official positions of the Counter-Terrorism Committee or any of its members.

Table of contents

PREMISE AND SCOPE OF REPORT

The present report was prepared by the Counter-Terrorism Committee Executive Directorate (CTED)[1] in accordance with Security Council resolution 2395 (2017), which reaffirms the essential role of CTED within the United Nations to identify and assess issues, trends and developments relating to the implementation of Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2322 (2016), 2396 (2017), and other relevant resolutions. Council resolution 2395 (2017) also recognizes CTED's relationships with, inter alia, academia; think tanks; and international, regional and subregional organizations, and notes their value in promoting an analysis of emerging threats, trends and developments.

Terrorist and violent-extremist groups have become increasingly adept at exploiting information and communications technologies (ICT) to promote their ideologies, recruit, and prepare attacks. In accordance with the relevant Security Council resolutions, the Counter-Terrorism Committee and CTED assist Member States to address the abuse of ICT by terrorists and terrorist groups.

In its resolutions 2322 (2016)[2], 2331 (2016), 2341 (2017) and 2396 (2017)[3], the Security Council calls on States to collect and preserve digital evidence so that investigations and prosecutions may occur to hold those responsible for terrorist attacks accountable. The present report seeks to provide counter-terrorism policymakers, practitioners, and experts with an overview of the current situation and challenges presented by a related trend and development: the state of international cooperation for lawful access to digital evidence.

The present report offers a snapshot of the regulatory reform landscape as of late 2021. It does not purport to be a full accounting of domestic legislation relating to data sharing or privacy. Although CTED recognizes that many Member States are currently introducing, or have already introduced, legislation and regulations on access to, control of, and the sharing of data in the domestic context, this report is focused on several key initiatives with broad impact — whether due to the size of the on-line market, the volume of Internet users affected, or the cross-border nature of the initiative.

---

[1] Guided by Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), and other relevant resolutions, the Counter-Terrorism Committee works to strengthen the capacity of United Nations Member States to prevent terrorist acts, both within their borders and across regions. The Committee was established in the wake of the 11 September 2001 terrorist attacks against the United States and is assisted by the Counter-Terrorism Committee Executive Directorate (CTED), which carries out the policy decisions of the Committee, conducts expert assessments of Member States, and facilitates the delivery of counter-terrorism technical assistance.

[2] Security Council resolution 2322 (2016) notes the significant increase in requests for cooperation in gathering digital data and evidence from the Internet. It also directs the Counter-Terrorism Committee, with the support of CTED, to identify gaps or trends in current international cooperation among Member States, including through Committee briefings to exchange information on good practices, and facilitate capacity-building, including through sharing good practices and exchange of information in this regard.

[3] Council resolution 2396 (2017) recognizes the challenges faced by Member States in obtaining admissible digital evidence and encourages Governments and the private sector to strengthen their cooperation in that regard. It further recalls its decision in resolution 1373 (2001) that Member States shall afford one another the greatest measure of assistance in connection with criminal investigations or proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings, and further underscores that this includes physical and digital evidence.

The report is also not a normative assessment of the various initiatives underway, nor a comprehensive account of the issues associated with cross-border law enforcement access to data. Instead, it is a status update with respect to a rapidly evolving and urgent problem. The report's main objective is to outline some of the key initiatives and to identify some of the major trends that contribute to the current overall cross-border situation in this area.

The report is based on information collected from various sources, including Member States' law enforcement authorities, privacy- and data-protection agencies, and representatives of the private sector and civil society organizations (CSOs) from around the world, as well as members of relevant international and regional institutions working on cross-border data reforms.

EXECUTIVE SUMMARY

Information collected by CTED and research shows that criminal evidence is increasingly electronic and often stored abroad. Consequently, routine domestic law enforcement investigations regularly include a cross-border element. The last few years have seen important developments in this area at the global, regional, and national levels. Despite these developments, the state of international cooperation to ensure timely access to cross-border evidence for law enforcement is insufficient. Many States rely on mutual legal assistance (MLA) treaties, which is a cumbersome and slow diplomatic solution that is ill-suited to deal with most electronic evidence requests.

Consequently, and as described in this report, Member States and international and regional organizations have pursued a variety of strategies to ensure that law enforcement agencies have lawful access to foreign-held data.

There are currently several major reform initiatives under way to ensure that law enforcement authorities have access to foreign-held data. In addition to regional initiatives such as that of the European Union and major reforms being introduced in States such as Brazil, China, India, the Russian Federation, and the United States, there are two major multilateral initiatives: the draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and the recently adopted Second Additional Protocol to the Council of Europe Convention on Cybercrime ('Budapest Convention") on enhanced co-operation and the disclosure of electronic evidence.

Each of these initiatives promises to resolve some aspect of the problems associated with access to electronic evidence. However, as is often the case when there are multiple reform efforts under way, there is a chance of fragmentation and the establishment of several competing and overlapping regimes on cross-border evidence. There are also concerns about a potential reduction in protections for basic human rights, including due process, freedom of expression, and privacy, which must be addressed in step with reform efforts.

The key challenges going forward will therefore include ensuring interoperability between the various initiatives and expanding the capacity of law enforcement agencies faced with a series of new transnational regulatory regimes. This is therefore a moment of opportunity for global and regional institutions, as well as private and multistakeholder groups, to expand capacity-building efforts aimed at addressing these challenges.

INTRODUCTION

Terrorists and violent extremists are increasingly using information and communications technologies (ICT), including the Internet and social media, to promote distorted narratives to justify violence, radicalize and recruit supporters, mobilize resources, and plan attacks. This process has been exacerbated during the COVID-19 pandemic.

However, in exploiting ICT, terrorists and violent extremists leave traces of their activities in the form of digital data that, if adequately tracked and processed, can become extremely valuable electronic evidence.

Digital data stored by service providers can prove where a crime was committed, disclose incriminating communications, and determine the location of offenders. Obtaining this digital evidence (electronic evidence or "e-evidence") can ensure that the right individual is prosecuted and that those who perpetrate serious offences are brought to justice. This makes the practice of lawfully obtaining digital evidence from online service providers an increasingly crucial element of successful prosecutions.

Recent terrorist attacks have demonstrated the need for immediate responses to emergency incidents, preservation of data, and urgent requests for international cooperation. Consequently, the number of requests for data made to private companies and through MLA channels to other States has increased exponentially.

However, current practice indicates that counter-terrorism investigators and law enforcement agencies continue to face challenges in collecting relevant digital evidence, for two primary reasons: first, because the evidence is very often in the online or cloud-based[4] possession of an Internet company, platform, or service provider, and second, because the transnational nature of the Internet means that digital data concerning a crime or its perpetration is often accessible only in a jurisdiction other than that in which the crime being investigated was committed.

For example, an investigator in State A might seek criminal evidence held by a foreign technology company that is headquartered in State B but stores its customer data in State C. This means that investigators seeking evidence of terrorism and other serious crimes must regularly seek cross-border access to data. This cross-border networking necessarily implicates the equities of each country involved, including their interest in the suspect, the crime, the data requested, the privacy rights of anyone connected to the data (including victims), and other concerns. This of course raises many diplomatic, jurisdictional, and practical challenges.

[4] "The cloud" refers to servers that are accessed over the Internet and the software and databases that run on those servers. Cloud servers are located in data centres all over the world.

Although this is an urgent problem, it is not entirely new. For several years, reports have recognized the difficulty of cross-border digital evidence collection.[5] Moreover, a number of regulatory initiatives have been implemented to address the situation. Some are State-led, formal and informal initiatives, which seek to coordinate State conduct around the globe. Others, like the Internet & Jurisdiction Policy Network, are informal and multistakeholder initiatives.[6]

The present report consists of three sections. The first section considers several major reform efforts currently under way, including the draft United Nations convention on cooperation in combating information crimes and the recently adopted Second Additional Protocol to the Budapest Convention, as well as the proposed European Union e-Evidence regulation, which is currently making its way through Europe's trilogue political process, the United States CLOUD Act, and other initiatives being developed in Brazil, China, India, and the Russian Federation.

The second section considers notable trends — developments that are relevant to the coordinated global resolution of the cross-border data problem — and challenges for the future. Among those trends is the increase in localization efforts, whereby States seek to ensure that some aspect of a foreign technology service provider is local (e.g., data storage, representative, or bank account) in order to ensure swift compliance with local law enforcement requests. Another notable trend is the fragmentation of the global effort to address cross-border data access. There are several major initiatives that attempt to resolve the associated issues. Although each of these initiatives on its own is important, collectively they represent an increasingly complicated set of instruments that add complexity to a problem that is already quite complex. Future investigators will need to navigate a complex web of different regulatory frameworks in order to determine the rules and normative frameworks, including for compliance with international human rights laws, that will apply to any given law enforcement data request.

The third section identifies several future policy goals aimed at addressing the challenges outlined in the second section. **Those goals include ensuring interoperability between the various regimes and expanding capacity, while ensuring respect for human rights and fundamental freedoms. Law enforcement agencies will always face jurisdictional hurdles in a global environment, but capacity-building and interoperability will reduce unnecessary delays in solving some of the most pressing investigations.**

---

[5] Global Network Initiative Report, *Data Beyond Borders: Mutual Legal Assistance in the Digital Age*, (2016), https://globalnetworkinitiative.org/wp-content/uploads/2016/12/GNI-MLAT-Report.pdf.

[6] The Internet & Jurisdiction Policy Network is a multistakeholder organization created to address the tension between cross-border Internet and national jurisdictions. Its Secretariat facilitates a global policy process engaging with over 400 key entities from Governments, the world's largest Internet companies, technical operators, civil society groups, academia, and international organizations from over 70 States. https://www.internetjurisdiction.net.

I. MAJOR REFORM EFFORTS

There are several significant reform efforts currently under way. Two of these are global in nature and aspire to cover a wide swath of the world's data requests. State and regional initiatives are just as consequential. Although these initiatives may cover only a single State, bilateral agreements, or a regional jurisdiction, they will nevertheless impact a significant number of Internet users. There are also significant reform efforts taking place within multistakeholder institutions. Each of these initiatives is at a different stage of development and each addresses an important need. But each also creates a new layer of complexity to the cross-border data situation.

A. Multilateral initiatives

(a) Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

The most recent of the major global initiatives to move forward is also the most wide-reaching. On 27 December 2019, the United Nations General Assembly adopted a resolution, based on a report of its Third Committee, to develop "an open-ended ad hoc intergovernmental committee of experts, representing all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes".[7] In May 2021, during its seventy-fifth session, the Assembly adopted a resolution outlining a path forward for the proposed convention. By the terms of the resolution, the Ad Hoc Committee will convene at least six sessions of 10 days each, to commence in January 2022, and submit a draft convention to the Assembly at its seventy-eighth session, in 2023.[8]

The full text of the draft convention was published in July 2021.[9] The draft convention aims to "promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of ICT" and "to improve the efficiency of international cooperation and to develop such cooperation, including in the area of personnel training and the provision of technical assistance for preventing and combating ICT crimes".[10]

The draft convention outlines a number of offences relating to, inter alia, drugs, terrorism, extremism, and child pornography that States Parties would be obligated to criminalize through domestic legislation. It also clarifies the kinds of data retention and criminal due process required for electronic evidence. Its article 36, for example, sets forth the requirement that each State Party implement domestic legislation to enable a production

---

[7] https://www.un.org/press/en/2019/ga12235.doc.htm.
[8] UN press release, *General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations* (26 May 2021), available at: https://www.un.org/press/en/2021/ga12328.doc.htm.
[9] Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, unofficial English translation available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf.
[10] *Ibid.*

order that would allow law enforcement authorities to compel "A person in its territory to provide specified electronic information in that person's possession or control" and to compel a service provider "offering its services in the territory of that State Party to submit subscriber information in that service provider's possession or control".[11]

Importantly, the draft convention emphasizes that it seeks to maximize international cooperation with regard to electronic evidence and act as a kind of multilateral Mutual Legal Assistance Treaty (MLAT) for States that do not already have an applicable MLAT in place. Article 52 of the draft convention outlines a series of procedures whereby each State Party designates a central authority for handling MLA requests and designates the Secretary-General of the United Nations as the central registry for tracking the contact information of those authorities. The draft convention also requires, pursuant to its article 66, that each State Party designate a point of contact for prompt cross-border assistance, a similar arrangement to the G7 24/7 Cybercrime Network *(see below)*.

In terms of implementing the proposed global treaty, the draft convention calls for the creation of a Conference of States Parties, as well as an International Technical Commission which, pursuant to article 79, "shall be a permanent body, consisting of 23 members and shall be created on the basis of the principles of mixed representation: two thirds of the members shall represent the Conference of the States Parties, and one third shall represent the governing bodies of the International Telecommunication Union (ITU)".[12]

(b) Council of Europe: Second Additional Protocol to "Budapest Convention"

The Council of Europe's Budapest Convention was the first international treaty aimed at tackling cybercrime and remains the most widely-ratified cybercrime treaty in effect today. The Convention was drafted 20 years ago and has grown to include 66 States Parties and 23 observer States and organizations from the European Union and worldwide.[13] However, the Convention was drafted before the rise of today's global computer systems and did not anticipate the dramatic increase in the number of cross-border law enforcement requests for data. For that reason, in 2012, an expert group (now known as the Cloud Evidence Group) was formed to study the issue and recommended updating the treaty with a Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence (commonly referred to as the Second Additional Protocol).[14]

After several years of negotiations, the Second Additional Protocol was adopted by the Committee of Ministers on 17 November 2021 with the aim of enhancing cooperation between State parties, improving the disclosure of electronic evidence for the purpose of

---

[11] *Ibid*.
[12] *Ibid*.
[13] https://www.coe.int/en/web/cybercrime/parties-observers.
[14] *Enhanced International Cooperation on Cybercrime and Electronic Evidence: Towards a Protocol to the Budapest Convention, Council of Europe* (5 September 2019), https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07.

specific criminal investigations and proceeding, and increasing the ability of law-enforcement authorities to counter cyber- and other crime, while fully respecting human rights and fundamental freedoms.[15] The Protocol provides a legal basis for disclosure of domain name registration information and for direct cooperation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate cooperation in emergencies, mutual assistance tools, as well as personal data protection safeguards. The text is expected to be opened for signature in May 2022.[16]

The Protocol has a number of consequential features. Most importantly, it will alter how law enforcement requests for data occur for States Parties. The biggest change — and the one that has inspired the most controversy — will be to allow States Parties to make direct requests to a service provider for subscriber information, even if that service provider is in another State. Subscriber information is defined to include "any information contained in the form of computer data […] relating to subscribers of its services other than traffic or content data", which includes subscriber identity, location, telephone and other contact details, payment information, and more.[17] This provision would constitute a major change for investigators in many States because it would allow them to bypass the formal MLA process and make direct requests to foreign technology companies, albeit for the more limited set of basic subscriber information.

Another significant feature of the Protocol is the procedure for receiving States to give effect to requests. This process effectively creates expedited MLA between member States. It would obligate receiving States to treat incoming requests for both basic subscriber information and traffic data as domestic requests. The request (along with supporting information, including factual evidence supporting the request) is not made directly to foreign technology service providers but rather to the competent authority to compel that service provider to produce the relevant data. The receiving country must take reasonable steps to give effect to the request, specifically by ordering the service provider in its jurisdiction to produce the relevant data in 20 days (for basic subscriber information) or 45 days (for traffic data).[18]

The Protocol also allows for expedited MLA requests in cases of emergency, which are defined as "a situation in which there is a significant and imminent risk to the life or safety of any natural person".[19] These emergency situations are understood to include imminent

---

[15] https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b.
[16] https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe.
[17] Paragraph 93, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol, V. 3, as approved by the T-CY at its 24th Plenary (28 May 2021). Also, see e.g., "Joint Civil Society Response to the Provisional Draft Text of the Second Additional Protocol to the Budapest Convention on Cybercrime," Electronic Frontier Foundation (EFF), European Digital Rights (EDRi), IT-Pol Denmark, and Electronic Privacy Information Center (EPIC) (Nov. 7, 2019), https://www.eff.org/document/eff-comments-additions-budapest-protocol-cybercrime.
[18] Art. 8, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol, V. 3, as approved by the T-CY at its 24th Plenary (28 May 2021).
[19] Art. 3(2)(c), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol, V. 3, as approved by the T-CY at its 24th Plenary (28 May 2021).

threats to critical infrastructure and post-terrorist attack scenarios, among other cases.[20] The process for such a request is fairly straightforward: the requesting country sends the emergency request to the receiving country through their respective 24/7 points of contact, as set out in the Budapest Convention. The requesting country must provide evidence that establishes that a genuine emergency exists and explain why the assistance being requested is necessary for addressing the emergency. If the receiving country agrees that there is an emergency, the electronic evidence on request can be provided as quickly as possible.

B. Regional and State-led initiatives

Of course, major global initiatives are not the only reform efforts under way. There are also a number of regional (multi-lateral), bilateral, and national (domestic) initiatives that are both consequential and noteworthy. The following examples are six among many that merit further study. The aim of this overview is to give a brief sense of recent developments and changes that are newly in effect and yet on the horizon.

(a) European Union: e-Evidence regulation

Over the past decade, the European Union has undertaken a major regional effort to establish a unified pan-European approach to electronic evidence. In April 2018, the European Commission proposed new rules in the form of a Regulation[21] and a Directive.[22] The Commission has stated that the proposed new rules are designed "To make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists".[23] The European Union e-Evidence Regulation was drafted to create a European Production Order, a European Preservation Order, include safeguards for the right to protection of personal data, and was envisaged to improve legal certainty and clarity concerning legal requests for data. The proposed Directive set forth obligations for service providers to designate a legal representative in the European Union for the receipt of, compliance with, and enforcement of decisions and orders.[24]

The signature piece of the Regulation was the creation of a new European Production Order that would allow "a judicial authority in one Member State to obtain electronic

---

[20] As per the explanatory report, paragraph 42: "situations involving "a significant and imminent risk to the life or safety of any natural person" may involve, for example … immediate post-terrorist attack scenarios in which authorities seek to determine with whom the attackers communicated in order to determine if further attacks are imminent; and threats to the security of critical infrastructure in which there is a significant and imminent risk to the life or safety of a natural person. Available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b.

[21] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

[22] 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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.

[23] European Commission, *E-Evidence – Cross-Border Access to Electronic Evidence,* https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

[24] Many service providers already designate a local legal representative based on Article 27 of the European Union's General Data Protection Regulation (GDPR), https://gdpr.eu/article-27-representatives-of-controllers-not-in-union/.

evidence (such as emails, texts or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another EU country." [25] Whereas the Second Additional Protocol to the Budapest Convention allows direct requests for subscriber information only, the European Union e-Evidence Regulation would allow for direct requests of stored content and non-content data, including traffic data.

The Production Order would also significantly shorten the time allowed for service providers to respond to requests. Whereas the current European Investigation Order (EIO)[26] requires a response withing 120 days with MLA processes taking an average of ten months, the proposed European Production Order will oblige service providers, or their legal representatives, to respond within 10 days, and with 6 hours in cases of emergency.[27] It is important to note, however, that the draft Regulation, per Article 23, does not seek to overwrite EIOs or prevent Member State authorities from issuing them to obtain electronic evidence.[28]

The proposed new rules also foresaw the creation of a European Preservation Order, which would allow a judicial authority in one EU country to request that a service provider, or its legal representative, in another EU country preserves specific data – preventing its removal, deletion or alternation for a period of 60 days – in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order.

The e-Evidence regulation would mark a significant change in the way that requests are handled within Europe and will certainly also have a significant impact outside Europe. For example, in February 2019, the European Council authorized the opening of negotiations between the United States and the European Union for simplified trans-Atlantic law enforcement requests. One of the challenges to reaching such an agreement is the need to ensure that any transatlantic deal satisfies the requirements set forth in the U.S. domestic CLOUD Act and in the e-Evidence Regulation, if and when it comes into effect. [29]

A draft report of the European Parliament Committee on Civil Liberties, Justice and home Affairs (LIBE) presented in November 2019 recommended changes to the proposed

---

[25] *Ibid.*

[26] In the European Union, the European Investigation Order (EIO), introduced by Directive 2014/41/EU, is the current mutual recognition tool used for cross-border requests related to all types of evidence.

[27] European Commission, *E-Evidence – Cross-Border Access to Electronic Evidence,* https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

[28] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Article 23: Relationship to European Investigation Orders – This provision clarifies that the Regulation does not prevent Member State authorities from issuing European Investigation Orders in accordance with Directive 2014/41/EU to obtain electronic evidence.

[29] The need for an agreement on the regulation of data flow between the European Union and the United States, in particular, bears extra weight since the July 2020 decision of the Court of Justice of the European Union in *Data Protection Commissioner vs. Facebook Ireland Limited, Maximilian Schrems ("Schrems II")* to invalidate the European Union – United States Privacy Shield that was previously used to facilitate data flow between the two jurisdictions. For further details, see: https://bigid.com/blog/schrems-ii and https://www.privacyshield.gov/welcome.

Regulation and Directive. On 7 December 2020, the LIBE Committee voted to adopt the report, signing off on the final text for the e-Evidence Regulation.[30] On 10 February 2021, trilogue negotiations began between the European Parliament, the European Council, and the European Commission. As of October 2021, reporting indicates the trilogue discussions are advancing, with agreement that the notification obligation of receiving member State authorities will only include cross-border data access orders to content and real traffic data. There is, reportedly, no consensus yet regarding the grounds for refusal of cross-border data access orders.[31] The result of continuing negotiations will determine the final scope and impact of the regulation.

(b) Brazil: Marco Civil da Internet

Brazil's signature Internet regulation, Federal Law No. 12.965/2014, the Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*), "[e]stablishes the principles, guarantees, rights and obligations for the use of Internet in Brazil".[32] Often referred to as the "Internet Constitution" in Brazil, the Marco Civil sets forth rights and guarantees for those who use the Internet and sets guidelines for State action.

The law, much like the European Union's proposed e-Evidence regulation, authorizes law enforcement to make direct requests to service providers operating in the country. Thus far, the Act has been used to compel foreign Internet Service Providers (ISPs) to provide relevant criminal evidence to law enforcement, and many fines have been levied against foreign service providers for noncompliance. But those providers have also been extremely active in fighting those fines in court. Facebook, for example, challenged the constitutionality of the Act. Its case is pending in the Brazilian Supreme Court.[33]

Additionally, Brazil's first general data protection law, the *Lei Geral de Proteção de Dados* (LGPD), entered into effect on 18 September 2020, with administrative sanctions for non-compliance entering into force in August 2021. The law covers the activities of data controllers and processors and creates requirements for the processing of information of data subjects.

Modelled on the European Union's General Data Protection Regulation (GDPR)[34], the LGPD has extraterritorial effect. Companies therefore do not need to have a physical presence in Brazil for the law to apply. If a company processes personal data in Brazil,

---

[30] The LIBE Committee further voted to reject the Commission's proposed Directive and instead integrate the relevant provisions on the appointment of legal representatives within the EU directly into the proposed Regulation. For further details, see: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf.

[31] EU policy update October 2021. https://centr.org/news/eu-updates/october-2021.html.

[32] Marco Civil Law of the Internet in Brazil, Law No. 12.965, 23 April 2014. In Portuguese and English: https://publicknowledge.org/policy/marco-civil-english-version/.

[33] Lourdes Pavioto Carreo v. Facebook do Brasil LTDA. in 2018, the Supreme Court agreed to consider an appeal filed by Facebook Brasil on the constitutionality of article 19 of the Marco Civil. https://wilmap.stanford.edu/entries/lourdes-pavioto-correa-v-facebook-do-brasil-ltda.

[34] The General Data Protection Regulation (GDPR) is a strict privacy and security law adopted by the European Union, which imposes obligations on any organization targeting or collecting data related to people in the European Union. The regulation was put into effect on 25 May 2018. It levies harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

processes personal data collected in Brazil, or processes personal data to offer goods or services in Brazil, then it will fall under the jurisdiction of the law. User rights provided by the LGPD go beyond those provided in the GDPR with respect to user access to information about who holds and has received their data.

The LGPD includes provisions on the appointment of Data-Protection Officers, Data-Protection Impact Assessments, record-keeping, data breaches, and the establishment of the Brazilian Data Protection Authority (ANPD). It also contains several requirements for the transfer of data using valid legal transfer mechanisms. Although organizations may transfer personal data to other State that provide an "adequate level of data protection," Brazil has not yet defined this. The two main ways in which organizations can transfer data are: (i) with the specific and express consent of the individual, and (ii) through contractual instruments which commit the organization to comply with the LGPD principles, individual rights, and the Brazilian data-protection regime.[35]

The law is in the nascent stages of implementation. The ANPD has just been established and a National Council for the Protection of Personal Data and Privacy (CNPD), tasked with the formulation of guidelines for the application of the data protection rules, was announced only in August 2021.

(c) China: Data Security Law and Personal Information Protection Law

China has adopted three main laws dealing with data security. Its 2017 Cybersecurity Law is aimed particularly at service providers and network operators and gives the Government broad authority to regulate online activities. The Law creates a set of strict guidelines for network operators to manage cybersecurity incidents, including record-keeping and reporting to, and working with, government agencies in national security or criminal investigations.

In 2021, two new laws dealing with data security and privacy came into force, providing added specificity about data localization, data protection, and data-export requirements.

China's Data Security Law (DSL), aimed at protecting national security interests in the usage, collection and protection of data, took effect on 1 September 2021. Pursuant to the 2017 Cybersecurity Law, the DSL sets up a framework for classifying data collected and stored in China depending on how it may harm national security, public interest, or social order. The Law establishes a tiered system of data-protection obligations, with the most stringent requirements reserved for "important data" (the scope of which is currently undefined but will have significance going forward).

The DSL has broad coverage and affects almost all organizations doing business in China. It covers the storage, use, disclosure, and processing of data within the territory of China and also extraterritorially if the data activities are deemed relevant to China's

[35] https://www.natlawreview.com/article/brazil-s-comprehensive-privacy-law-now-effect.

national security and public interest. Requirements for companies engaged in data processing within China include basic cybersecurity hygiene (including security training and upkeep); the conducting of periodic risk assessments vis-à-vis "important data"; the reporting of potential risks to relevant government bodies; and the designation of a responsible data-security person and/or department.

Notably, in the context of the present report, the DSL significantly tightens the restrictions on transfer of data outside China. In particular, it expressly prohibits provision of any data stored in China — regardless of the data's classification level or whether the data was initially *collected* in China — to any foreign judicial or law enforcement agency without the prior approval of the relevant government authorities.[36]

The penalties for violating the Law are significant. Companies found in violation of regulations concerning "core data" face penalties of up to RMB 10 million (c. $1.56 million), the forced shutdown of their businesses, and potential criminal liabilities. Companies found in violation of regulations concerning "important data" face penalties of up to RMB 5 million (c. $780,000).[37]

China's new Personal Information Protection Law (PIPL) took effect on 1 November 2021 and applies to all types of data activities involving the personal information of data subjects in China, as well as activities outside China that are aimed at providing products or services to individuals in China or analysing their behaviour. The Law requires that cross-border data transfers be submitted first to the Cyberspace Administration of China (China's cyber- and data-protection regulator). The Law stipulates sanctions for non-compliance, including fines of up to RMB 50 million (c. $7.78 million).[38]

Much like the European Union's GDPR, the PIPL has extraterritorial effect and aims to impose limits on the collection of data about Chinese citizens, within China and abroad. It focuses on personal information, which it defines as information recorded in electronic or other means relating to an identified or identifiable natural person. The PIPL imposes obligations on data handlers relating to consent, data collection, and deletion, and sets volume thresholds for the triggering of data-localization requirements and the requirement for the appointment of an information protection officer to supervise the handing of data. There are also restrictions on the transfer of personal information to third parties and overseas.

(d) India: Personal Data Protection Bill 2021

In December 2019, India introduced the Personal Data Protection Bill, which underwent a number of amendments in a Joint Committee of Parliament (JCP) review process. The JCP adopted the final report on the Bill in late November 2021 and the amended Data

---

[36] https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws.
[37] *Ibid.*
[38] https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws.

Protection Bill 2021 (PDPB 2021) will now move towards adoption. This Bill has long been anticipated and will be closely watched, given India's massive on-line market.

The PDPB 2021 is a comprehensive privacy law which covers a range of issues and aims to align India's data-protection regime with the European Union GDPR. The Bill establishes protections on the cross-border flow of data and includes the creation of a Data Protection Authority (DPA).[39] However, there are some key differences. The PDPB 2021 will require only "significant" data fiduciaries (data controllers), instead of all data controllers and processors, to maintain records of processing activities. The scope of the Bill is likely to be broader than the GDPR as it will "include the processing of personal data by the State, any Indian company, any citizen of India, or any person or body of persons incorporated or created under Indian law".[40]

Among other things, the PDPB 2021 contains provisions on both personal and non-personal data.[41] This has generated criticism from experts who question whether the Government may gain overarching powers from the inclusion of non-personal data in the Bill. The Government of India may also exempt government agencies from the rules of the PDPB 2021 on the grounds of national security, public order, sovereignty, and other reasons.

The PDPB 2021 also requires that "critical personal data" must be stored and processed only in India. This could give the Government a vast mandate to force local data storage for a broad set of data types. The Bill also requires that "sensitive personal data" be stored in India, although it can be copied and processed elsewhere under certain conditions.[42] Notably, India's Bill follows the GDPR's adequacy requirement: "In order for data to be copied into a country, the destination country must apply sufficient privacy protections to the data and not impede Indian law enforcement access to the data".[43]

In terms of sanctions for non-compliance, the penalties under the GDPR and PDPB 2021 are similar, with fines of up to 4 per cent of global annual revenue. The PDPB 2021 also includes criminal liability provisions. Of note, the report of the JCP recognized that the parent company of social media platforms should set up an office in India and be regulated in order to be allowed to operate.

The next steps depend on how quickly the Bill will be tabled in Parliament and pass both houses to become law. The Bill introduces a sunset clause which will provide a two-year delay, after it is signed into law, for the rules to come into effect.

---

[39] https://f.hubspotusercontent10.net/hubfs/5214163/Whitepapers%20and%20Data%20Sheets/Guide%20to%20Indias%20Personal%20Data%20Protection%20Bill%20(PDPB)%20(1).pdf.

[40] *Ibid.*

[41] The PDPB 2021 includes an individual's name, mobile telephone number, biometrics, and other identifying information as personal data. Non-identifying information is considered non-personal.

[42] Personal Data Protection Bill, 2019, Bill No. 373 of 2019, art. 33 "Restriction on Transfer of Personal Data Outside India", available at: https://drive.google.com/file/d/1vmeCRehq7eiURstOhnio_UTaCkSgM5gv/view.

[43] Arindrajit Basu & Justin Sherman, *Key Global Takeaways from India's Revised Personal Data Protection Bill*, LAWFARE (23 January 2020), https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill.

(e) Russian Federation: Data-Localization Law

The Russian Federation has introduced several important laws regulating data handling, processing, and transfer that are relevant to cross-border law enforcement access. The most significant of those laws, for the purposes of the present report, is known as the Data-Localization Law (Federal Law No. 242-FZ Amending Certain Legislative Acts Concerning Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks), which was signed on 21 July 2014 and took effect in late 2015.

The Data-Localization Law requires:

> [A]ll data operators to ensure that any recording, systematization, accumulation, storage, change, or extraction of Russian citizens' personal data occurs in data centers located in Russian Federation territory. This means that any Russian citizens' personal data that data operators collect must be stored in servers, IT systems, databases, or data centers located in Russia.[44]

This provides greater control over online content and communications and allows for extrajudicial access to user information. Importantly, the Law does not impose restrictions on cross-border data transfers. The Federal Service for Supervision of Communications, Information Technology, and Mass Media (*Roskomnadzor*) has been increasingly active in enforcing the localization law, including by levying fines against service providers for refusing to store Russian citizens' data in Russia.[45]

This localization mandate is designed in furtherance of Russia's core data-protection law, the Russian Federal Law on Personal Data (Federal Law No. 152-FZ), which took effect on 27 July 2006 and creates the broadest responsibilities for service providers and data operators to take "the necessary organizational and technical measures required for protecting personal data against unlawful or accidental access". On 1 March 2021, amendments to the Personal Data Law went into effect as part of a legislative package that also involves the amendment of the Criminal Code to criminalize disclosure of personal data about "protected persons" (several categories of government officials).[46]

Like the European Union's GDPR, Russia's Personal Data Law has broad extraterritorial reach. It appears to cover data processing that occurs or is targeted at the Russian territory but also covers the collection or Russian citizens' personal data, as well as cross-border transfers of that data.

---

[44] https://www.gorodissky.com/publications/articles/data-protection-in-the-russian-federation-overview-tr2020/.

[45] Facebook has been fined 15 million rubles ($202,000) and Twitter has been fined 17 million rubles ($229,000). WhatsApp received a separate fine of 4 million rubles ($54,000), according to a statement from Russian internet regulator Roskomnadzor. https://globalvoices.org/2021/08/26/russian-court-issues-bigger-fines-to-social-media-companies-for-breaching-data-localization-rules/.

[46] https://fpf.org/blog/russia-new-law-requires-express-consent-for-making-personal-data-available-to-the-public-and-for-any-subsequent-dissemination/.

To further enhance its data-localization law, Federal Law No. 236-FZ "On the Activities of Foreign Entities in the Information and Telecommunications Network "Internet" in the Russian Federation" came into force on 1 July 2021. The Law affects two groups of foreign companies, such as social networks, messengers, audio-visual and gaming services, and search engines. The first group includes owners of information resources with a daily audience in Russia of at least 500,000 people. The second group includes foreign entities that are hosts and administrators of Internet resources aimed at and visited by Russian users, and as determined by Roskomnadzor. A list of foreign companies subject to the law will be published on Roskomnadzor's website.[47]

Companies subject to Federal Law No. 236-FZ must register a personal account on Roskomnadzor's website, to be used to communicate with Russian State bodies, and install a programme for determining the number of users. Applicable companies must also open a branch, office or independent legal entity in the Russian Federation to represent the interests of the foreign company with Russian authorities and enforce decisions of Russian courts and state bodies. Sanctions may be applied by Roskomnadzor in the event of non-compliance.

(f) United States: CLOUD Act

In 2018, the United States Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amended the Stored Communications Act to allow U.S. law enforcement to compel data held by U.S. technology service providers regardless of the storage location including abroad.

In addition, the CLOUD Act authorizes the U.S. Government to enter into executive agreements with other States that meet certain criteria, whereby the United States and the partner State agree to remove legal impediments to cross-border compliance with legal orders in cases that involve serious crimes, including terrorism. Both States would be able to directly submit to Communication Service providers (CSPs) orders for electronic evidence needed to combat serious crime, without involving the other Government and without fear of conflict with the laws of the other State. Given that most of the biggest technology companies in the world are U.S.-owned and headquartered and that the majority of the most-used web services around the world are also U.S.-owned and headquartered, this domestic piece of legislation has considerable implications around the world.

There are fundamentally two sides to the CLOUD Act: (1) the authority it gives U.S. law enforcement over foreign-held data, and (2) the authority it gives (or denies) foreign entities over U.S.-held data.

---

[47] Legislation and other information available in English: https://www.cms-lawnow.com/ealerts/2021/07/russia-adopts-law-forcing-foreign-it-companies-to-land-in-the-country; in Russian: http://publication.pravo.gov.ru/Document/View/0001202107010014?index=34&rangeSize=1.

First, on the U.S. side, the CLOUD Act essentially resolves the problem that law enforcement had experienced in seeking access to evidence held in other States by U.S. service providers. This was the crux of the Supreme Court case *Microsoft v. U.S.* regarding law enforcement access to data held by Microsoft in the company's Irish datacentres. In that case, the U.S. Department of Justice claimed that U.S. access to evidence (pursuant to the Stored Communications Act) did not vary based on the location of data storage. The CLOUD Act codified this longstanding U.S. doctrine and practice.[48] Under the CLOUD Act, if the U.S. Government has jurisdiction over the entity that controls the data in question, it will compel companies subject to its jurisdiction — via warrant, order, or subpoena — to produce requested data that the company controls, regardless of whether the data is or was stored in the U.S. or on foreign soil.

Second, on the foreign side, the CLOUD Act authorizes the U.S. Government to enter into executive agreements with other States that meet certain criteria to allow those Governments to make direct requests of U.S.-held data. The CLOUD Act therefore effectively permits partner States to obtain the data directly from U.S. service providers. Those States that do not have a CLOUD Act agreement with the U.S. Government will need to seek the data some other way, either through MLA, judicial assistance, or some other mechanism (e.g., demanding data localization).

CLOUD Act agreements are limited to requests for information relating to the prevention, detection, investigation, or prosecution of serious crimes. Requests must follow legal process. Data subject to request can include data stored or processed by CSPs, such as the contents of communications, non-content information associated with such communications, subscriber information, and data stored remotely on behalf of a user in the cloud. Notably, the CLOUD Act requires that foreign government orders that are subject to an executive agreement may not intentionally target data of U.S. persons or persons located in the United States. The foreign Government is free in negotiations to seek similar restrictions that would prevent the United States from using orders subject to the agreement to target data of its nationals or residents.[49]

In the event that a U.S.-owned or headquartered company refuses to comply with a non-U.S. request, the penalties to be imposed are based on the law in the requesting country.[50] This has caused some tech companies to raise concerns about national legislation deemed to create "conflict of laws" scenarios that the CLOUD Act is meant to preclude.[51]

With respect to human rights protections, including the prohibition on arbitrary or unlawful interference with privacy, it should be noted that the CLOUD Act is consistent with the Budapest Convention. The CLOUD Act also allows for executive agreements to be concluded only with third States that have robust privacy and civil-liberties protections

[48] https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/.
[49] https://www.justice.gov/dag/page/file/1153466/download.
[50] https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/.
[51] https://www.zdnet.com/article/google-wants-australia-to-remove-civil-penalties-from-cloud-act-readying-bill/.

in place, including that orders under CLOUD Act agreements shall be subject to review or independent oversight.[52] Further, it does not permit bulk data collection.[53]

C. Other relevant initiatives

In addition to the above domestic and international legal reform efforts, there are an increasing number of individual national laws affecting data sharing and privacy (128 States have already implementing some form of data protection and privacy legislation[54] and others are actively drafting domestic laws).

There are also a broad range of collaborative and practical efforts under way. These are typically driven by multistakeholder groups — featuring industry, civil society, and government stakeholders — and are typically focused on capacity-building, networking, ideation, and coordination. The following are just a few of many examples.

(a) United Nations initiatives

(i) CTED-UNODC-IAP Global initiative

The United Nations — in particular CTED and the United Nations Office on Drugs and Crime (UNODC) — have played an important role in convening relevant experts to assess needs and develop shared good practices in the cross-border handling of digital evidence. Security Council resolution 2322 (2016) notes the significant increase in requests for cooperation in gathering digital data and evidence from the Internet. Council resolution 2396 (2017) recognizes the challenges faced by Member States in obtaining admissible digital evidence and encourages Governments and the private sector to strengthen their cooperation in that regard.

In an effort to assist States to address those challenges, CTED, together with UNODC and the International Association of Prosecutors (IAP), launched a Global Initiative [55] in December 2017 with the aim of strengthening the capacity of national institutions and officials to combat crimes committed through the use of ICT, particularly those involving electronic evidence, in an interconnected and holistic manner.

The Global Initiative has facilitated the development of practical tools specifically tailored to the needs of law enforcement and judicial authorities, building on the experience of national experts and practitioners. The most notable result of this close cooperation is

---

[52] *Ibid.*
[53] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act,* April 2019, pp. 2-3, 5, 13.
[54] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[55] "Strengthening the Capacity of Central Authorities, Counter-Terrorism Prosecutors and Investigators in Obtaining Digital Evidence from Private Communications Service Providers (CSPs) in Cross-Border Investigations, with a Particular Focus on Counter-Terrorism Matters".

the "Practical Guide for Requesting Electronic Evidence Across Borders", published first in 2018 and released in July 2021 in its updated second edition.[56]

The Practical Guide combines the knowledge and experiences of Member States, international and regional organizations, and private-sector service providers to assist criminal justice officials to identify steps at the national level to gather, preserve and share e-evidence, with the overall aim of ensuring efficiency in MLA and facilitating understanding of other types of measures, such as voluntary data preservation and disclosure. The second edition is being used to provide technical assistance to Member States around the world and map the practice of hundreds of service providers.

Two additional tools are the Data Disclosure Framework (DDF) and the Standardized Direct Request Forms (SDRFs). The DDF is a guide to introduce general practices developed by international service providers in responding to overseas government requests for data. It is the result of active engagement with service providers and aims to give start-ups, smaller tech companies, and micro-platforms the confidence to respond speedily and lawfully to requests for e-evidence in counter-terrorism investigations. The SDRFs are based on best practices and are intended specifically for preservation (non-emergency) voluntary disclosure and emergency disclosure requests sent to CSPs that lack their own format.[57]

To ensure compliance with international human rights, CTED and UNODC have mainstreamed human rights law into all activities and tools developed under the joint Global Initiative, integrating relevant jurisprudence and documents developed by United Nations human rights mechanisms, and working alongside the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism in the development of the Practical Guide and related tools.

(ii) UNODC

Separately, UNODC has launched the Electronic Evidence Hub,[58] a "one-stop window" for legal resources and practical tools on e-evidence, which encompasses relevant jurisprudence and national laws and hosts practical resources developed in cooperation with experts and practitioners. UNODC is also currently updating the 2007 UNODC Model Law on Mutual Assistance in Criminal Matters through the addition of provisions on electronic evidence and special investigative techniques.

---

[56] https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html.

[57] The 2021 "Practical Guide for Requesting Electronic Evidence across Borders" and related tools are available only to central and competent national authorities and Permanent Missions to the United Nations via https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html.

[58] https://sherloc.unodc.org/cld/en/st/evidence/electronic-evidence-hub.html.

(iii) Secretary-General's Roadmap for Digital Cooperation

Since 2018, the Secretary-General of the United Nations has undertaken a series of initiatives to explore issues relating to global digital cooperation in advancement of the United Nation's Sustainable Development Goals and in recognition of the need for all people to be connected, respected and protected in the digital age.[59]

In July 2018, the Secretary-General appointed a high-level panel to consider the question of "digital cooperation". The panel released its report and recommendations, "the Age of Digital Interdependence" in June 2019.[60] Recommendation 5 focused on global digital cooperation and contained a recommendation for an open consultation process to develop updated mechanisms for global digital cooperation and an improved cooperation architecture, as well as a statement of support for a multi-stakeholder "systems" approach for cooperation and regulation that is adaptive, agile, inclusive, and fit for purpose for the fast-changing digital age.

On 11 June 2020, the Secretary-General launched the Roadmap for Digital Cooperation,[61] which builds on recommendations made by the above-mentioned high-level panel. With input from Member States, the private sector, civil society, the technical community and other stakeholder groups, the Roadmap addresses how the international community can better harness the opportunities and effectively deal with challenges presented by digital technologies. An update from the newly-established Office of the Secretary-General's Envoy on Technology, issued on 27 April 2021, provides highlights of the work being conducted to implement the Roadmap.[62]

Although the Roadmap addresses a range of issues relating to digital cooperation (including digital human rights, digital identity, privacy, and data protection), it does not delve into specific areas of digital evidence or MLA for the collection of digital data to be used in law enforcement-related investigations.

(iv) UNOCT/UNCCT - INTERPOL Handbook

The United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) and the International Criminal Police Organization (INTERPOL) launched the second edition of the handbook on "Using the Internet and Social Media for Counter-Terrorism Investigations" in November 2021. The handbook contains good practices on understanding terrorists' current use of the Internet and social media, conducting online counter-terrorism investigations, and steps for

[59] https://www.un.org/en/sg-digital-cooperation-panel.
[60] United Nations General Assembly report (A/74/821), https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.
[61] https://undocs.org/en/A/74/821.
[62] https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Update_on_Roadmap_implementation_April_2021.pdf.

requesting the preservation and collection of electronic evidence, including from service providers. It also provides a comprehensive list of practical online tools.[63]

(b) SIRIUS Project

The European Union Agency for Criminal Justice Cooperation (Eurojust) and the European Union Agency for Law Enforcement Cooperation (Europol) co-implement the SIRIUS Project, which serves as a central reference point in the European Union for knowledge-sharing on cross-border access to electronic evidence. SIRIUS consists of a community of competent authorities from 44 States, representing all European Union member States and a growing number of third countries. The SIRIUS platform hosts IT tools, training materials, and guidelines of more than 40 online service providers (OSPs) for data disclosure based on voluntary cooperation and MLA. The project released its third annual SIRIUS EU Digital Evidence Situation Report in November 2021.[64]

(c) G7 24/7 Cybercrime Network

The G7 24/7 Cybercrime Network began under the auspices of the Group of Eight (G8)[65] with a handful of States and currently includes over 70 States. The idea for the Network began at a 1997 meeting of the G8 Justice and Interior Ministers and has grown steadily ever since, under the operation of the G7 "Roma-Lyon Group's High-Tech Crime Subgroup".

The Network is primarily used for emergency-data requests and data-preservation requests regarding electronic evidence (including, intra alia, email, web pages, and customer records). Because local ISPs often have some of this information, the Network has traditionally emphasized local ISPs. The protocol for the network is as follows:

> "To use this Network, law enforcement agents seeking assistance from a foreign Participant may contact the 24-hour point of contact in their own state or autonomous law enforcement jurisdiction, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign Participant. Participants in the Network have committed to make their best efforts to ensure that Internet Service Providers freeze the information sought by a requesting Participant as quickly as possible".[66]

The Network requires that all members appoint a single point of contact who will be available 24 hours a day, seven days a week, can communicate in English, and is knowledgeable in cybercrime matters. Whereas the other initiatives described here are

---

[63] The handbook is available only to law enforcement officers and related practitioners via their respective INTERPOL National Central Bureaus (NCBs).
[64] SIRIUS situation reports are publicly available at https://www.eurojust.europa.eu/sirius.
[65] Beginning in 1997, G8 members consisted of Canada, France, Germany, Italy, Japan, the Russian Federation, the United Kingdom, and the United States. The group became the G7 upon the exit of the Russian Federation in 2014.
[66] U.S. Department of Justice Presentation, *24/7 Cybercrime Network, https://rm.coe.int/1680303ce2*.

focused on policy, the 24/7 Network has been influential in coordinating international access to electronic evidence on the ground.

(d) Internet & Jurisdiction Policy Network

Another prominent global multistakeholder effort is the Internet and Jurisdiction Policy Network (I&JPN), a multistakeholder organization that addresses issues between national jurisdictions and the cross-border Internet.[67] The I&JPN engages with over 400 key entities from Governments, several major technology companies, civil society groups, academia and international organizations from over 70 States. It holds regular meetings and seeks to build capacity, coalesce expert networks, and develop novel policy ideas. In May 2020, the I&JPN conducted regional consultations on the future of the United Nations Digital Cooperation Architecture in the context of recommendation 5 of the Secretary-General's above-mentioned high-level panel.

Under its data and jurisdiction programme, the Network is seeking to enhance legal interoperability and develop regimes for cross-border access to electronic evidence. In 2021, the I&JPN released a Toolkit on Cross-border Access to Electronic Evidence, which outlines the ways in which data flows and privacy can be reconciled with lawful access requirements to address crime.[68]

II. TRENDS AND CHALLENGES

The challenges presented by criminal evidence stored in the "global cloud" infrastructure hosted by public providers are now well-known. It is reassuring that so many reformers around the world recognize the urgency of the problem and have acted to address it. There follows a brief account of some of the key trends and challenges relevant to those reform efforts. Whereas some are the reasons for the reform efforts, others are new challenges that have arisen precisely because of the reform efforts currently under way.

A. Legal fragmentation

The first obvious consequence of the growing number of reform efforts is increased fragmentation, which in turn means increased complexity. Where today's law enforcement officers must contend with an array of bureaucratic and diplomatic hurdles to navigate an MLAT request for foreign-held data, future law enforcement agents will need to navigate an often-overlapping array of new frameworks. The development of any reform initiative (let alone several major initiatives) will of course almost certainly enhance efforts to tackle the cross-border data problem. However, as new reforms develop, there is the risk that the regulatory regime will become fragmented and increasingly complex. States may elect to support one reform effort and not another, or

[67] https://www.internetjurisdiction.net/.
[68] https://www.internetjurisdiction.net/data/toolkit.

they may participate in more than one, leaving law enforcement to determine which, if any, regime's rules will apply in a particular scenario.

Fragmentation frustrates one of the key goals of the reform initiatives, which is to simplify an overly complex and fragmented set of jurisdictional concerns for accessing digital evidence. This is why some experts report major concerns about replacing one complicated multi-jurisdictional MLAT-for-data regime with a new, yet still very complicated, multi-jurisdictional regime.

One concern is the prospect that any new regime might merely shift the burden for requests from law enforcement agents from one State to another. This might "solve" the problem from the perspective of the first State, but risks creating a new problem for the second State. If the second State is not capable of handling the thousands of incoming requests, the cross-border e-evidence situation will be different, but not necessarily better.

B. Decreased interoperability

Related to the problem of fragmentation is the risk of decreased interoperability. Four reform efforts might be seen as better than one — one would think that the more regulatory coverage the better — but with so many initiatives under way, the challenges involved in ensuring their compatibility increase.

For example: suppose that law enforcement officers from France seek data held in Ireland and consider that both Ireland and France are subject to both the European Union e-Evidence regulation and the Second Additional Protocol to the Budapest Convention. Which agreement would govern? Suppose also that the French authorities sought data held by two States — one a party to the e-Evidence regulation and another a party to the Second Additional Protocol. These are resolvable issues and occur frequently where there is a fragmented and overlapping regulatory landscape, but investigators will need guidelines for navigating these new electronic evidence regimes. And requests under one regime will very likely not be interoperable with requests from a different regime.

As these reform efforts progress, each should endeavour to clarify any overlap with other regulatory initiatives. It would be even better if the major initiatives were to coordinate to ensure that requests under one format (e.g., the Budapest Convention's request format or the e-Evidence regulation's European Production Order) have an easily identifiable equivalence under the other reforms.

C. Localization

One natural response to the transnational legal problems raised by the global cloud has been for States to try to eliminate the "borderless" nature of cloud storage by controlling data residency. The greater degree to which the domestic Internet is local, the easier it is for law enforcement to regulate. By requiring foreign providers to store some or all data locally, the State can effectively mandate its way out of the cross-border problems.

Requiring data providers to localize legal representation by opening a local office or appointing local staff to supervise the handling of data is another measure States are exploring to localize data custody.

Localization is both a natural response to the global cloud and a challenge to it. It is natural in the sense that States, being tasked with regulating the local impact of the Internet, would seek to exert control over the service providers and services that make business and have an impact on their territory. This is the logic, and it is compelling: after all, this is the way that things work for non-Internet businesses, which typically need a local presence to market and sell their goods or services.

However, localization is also in a state of tension with the global cloud system because one of the very benefits of the global cloud is the idea that anyone could put a service online and that service would instantly be available around the world, including in other States. The proverbial start-up developer working at home is not expected to have local legal counsel or a local data-storage option. Requiring such developers to have local storage in every State where their services are offered might be prohibitive, especially as they start out.

There are several downsides of forced data localization and mandated local legal representation. Civil society groups and service providers have been the most vocal opponents of the idea of data localization, noting that the requirement for local data storage is often intended to reduce barriers to government access to user data. In that sense, data localization is regarded a threat to user privacy and human rights. It is also undoubtedly costly for service providers which, in some cases, must re-engineer their network services (which have been designed and optimized for a borderless global network), position specific staff, and/or open local offices in multiple locations.

The upsides of data localization and localized data custody are that they can reduce, and in some cases eliminate, the cross-border conflicts that arise because of the global cloud. For example: supposing that law enforcement agents in State A are investigating a murder there and seek digital evidence held by a company in State B. Currently, law enforcement agents from State A must request MLA from State B to compel the service provider to produce the relevant evidence required for State A's criminal investigation. If, however, State A were to adopt a law requiring foreign ISPs to respond to local requests directly — either by storing the data locally or simply having a legal representative or other means of responding to local requests — State B need not be involved at all and the local crime could be handed locally.

This has obvious appeal to Governments around the world, and a number of States have adopted their versions of rules for national data storage.[69] Some commentators have noted that it will continue to have such appeal even as the various reform efforts

[69] Australia, Canada, China, Germany, India, Indonesia, Kazakhstan, Nigeria, Russian Federation, Republic of Korea, the Kingdom of Saudi Arabia, Spain, the United Arab Emirates, Viet Nam, and other Member States, have national data localization laws already in force.

described in the present report are fully developed. This suggests that those reform efforts (whatever they achieve) may never fully eliminate the trend towards data localization.

D. International human rights concerns

The ways in which States address the management of digital evidence in counter-terrorism matters raises many critical human rights questions, including with respect to how States define the terrorism offence. Obtaining, storing, and exchanging such evidence could impact whether suspects are receiving fair treatment in accordance with principles of due process and the presumption of innocence and whether rights such as those to freedom of expression and privacy are properly safeguarded. In addition, protections provided in one State may not be guaranteed in others, raising the question of whether cooperation can proceed at all. These complex issues are presenting significant challenges to many States.

One common denominator across these various reform efforts is the concern expressed by civil society groups at a potential reduction in protections for basic human rights. As reform efforts expand information access, human rights activists have expressed concern that law enforcement authorities will gain too much access too quickly, without adequate consideration for, inter alia, international human rights and fundamental freedoms (including due process, the right to freedom of expression, and the right to privacy).

Because of the diplomatic nature of large multinational reform efforts, civil society groups also express concerns at the compromises that will be necessary to create uniformity. They fear a "lowest common denominator" dynamic whereby States will compromise on their privacy and due-process protections in order to achieve a universal electronic evidence standard. Agreeing on a common standard across States will almost certainly ultimately lead to a lower standard than one that would be achieved by identifying a high universal standard and asking States to "level-up". The concern is that, in order to address law enforcement's jurisdictional problems, the substantive law will become weakened, giving law enforcement too-quick access with too-little due process. The trend towards universalization, in other words, could lead to a lowest common denominator in terms of due process.

Fragmentation (i.e., the coexistence of several different legal regimes) also presents challenges with regard to respect for human rights. If, for example, law enforcement agencies were presented with options in pursuing data from two different States, they might elect the State with the fewest barriers to accessing the data. Another possibility is that, if States agree to lower standards for cross-border investigations than they apply at home, there may be pressure to lower the standard at home (since it would be odd if it were easier for foreign investigators than for domestic investigators to gain access to digital evidence in a given State).

Human rights groups also express concern at the use of national security investigations as a pretext for a range of human rights abuses. They fear that investigators might invoke counter-terrorism or cybersecurity needs in order to suppress lawful and protected speech or invade citizens' privacy.

E. Private-sector practice

The recipient of law enforcement data requests is typically a large technology firm, often one located in another jurisdiction. How that company handles law enforcement requests (i.e., what law it applies, what evidentiary showing it requires, what languages it recognizes, and so forth) can strongly influence the outcome of the request. Whether it is relevant to the lawful data request or not, the fact remains that the way in which service providers handle incoming requests is of enormous consequence, which has led to service providers having a quasi-judicial role in the provision of e-evidence across borders.

There is considerable diversity across the private sector in terms of how different service providers handle law enforcement requests for data. Large and small firms differ considerably in terms of their capacity and expertise in handling foreign law enforcement requests. The largest technology companies collectively handle hundreds of thousands of law enforcement requests for data every year. All major technology firms have developed settled and often well-understood processes for managing requests for data (even though those processes differ somewhat in structure). The smaller companies, however, generally have much less capacity for managing local law enforcement requests. A smaller ISP might not have a local representative in every jurisdiction in which it operates and might not even have staff who are knowledgeable about local laws and procedures. In some cases, smaller firms may not even have staff who can translate a law enforcement request written in another language.

There are of course many other differences, which depend on the location of the firm's headquarters, its overall culture, and so forth. This can mean that, for a given piece of data, much will depend on the service provider that holds that data. This is a point of frustration for law enforcement agents. Standardization across the industry could alleviate this problem, as would capacity-building at smaller firms. These are suitable objectives for multistakeholder initiatives and industry trade groups alike.

III. LOOKING AHEAD

Given that there are several major initiatives already under way and that, for the foreseeable future, they will probably co-exist, the focus for reformers and technical assistance providers for moving forward and addressing challenges should be to ensure interoperability and expand capacity for law enforcement agents navigating between the different regimes. It is also clear that ensuring respect for and compliance with

international human rights law and fundamental freedoms are necessary components of reform and capacity building efforts.[70]

A. Ensuring interoperability

Reformers — and those pushing reformers to make changes one way or the other — should seek to maximize interoperability and, just as importantly, clarify where one regime is or is not interoperable with another. It would be relatively simple to establish some forms of interoperability by ensuring that the same point of contact (whether an office or a person) is used for each regime. This would avoid the difficulty of having to find the right contact for the legal authority used to compel digital evidence. Similarly, interoperability would be strengthened if States were to develop similar forms for managing these requests. Even better are forms that clarify the limits of one requesting regime or another. (The UNODC model law project is a good example of this.)

One example of interoperability is the use of a universal request form. The problem of fragmentation would be greatly alleviated — and capacity-building efforts greatly enhanced — if each of the reform initiatives described in the present report were to develop a shared request form that could be used by all law enforcement agencies. A single form could guide law enforcement agencies towards one set of standards or another (depending on their respective States' membership) and would be understandable and actionable regardless of the legal authority invoked.

There is also a role to be played by the private sector. Service providers can — and sometimes do — help ensure a fairly uniform process for managing requests, regardless of the regime or legal framework involved. The notice given to the requesting officer, the person or persons whose data is being requested, where appropriate, and feedback about what kinds of requests are or are not complete can be implemented in a way that reduces the overall friction between different regimes. The above-mentioned CTED/UNODC DDF can alleviate some of these concerns by giving private service providers guidance on how to handle requests.

In terms of human rights in the context of requesting electronic evidence across borders, the United Nations International Covenant on Civil and Political Rights (ICCPR) Article 17 and the Universal Declaration of Human Rights (UDHR) Article 12, in particular, act as universal benchmarks on amidst the problem of fragmentation highlighted in this report, and those engaging in interoperability reform efforts should draw on these articles to ensure a clear baseline on privacy matters.

[70] Human rights particularly relevant to the requests of electronic evidence across borders are the right to privacy, the right to a fair trial, the recognition of a person before the law, non-discrimination, the freedom of opinion and expression, freedom of association, freedom of movement and freedom of religion or belief.

B. Expanding capacity

Capacity-building is essential. Despite the major initiatives under way, CTED's dialogue with Member states shows that significant portions of the world's law enforcement establishment continue to have little or no training on the basic rules governing the kind of process required for each type of digital evidence. All those involved — States, service providers, users, civil society — benefit when police make only requests that are lawful and guided through the appropriate channels. Moreover, the scale of the problem is so significant that capacity-building efforts are worthwhile even for the largest and most well-resourced States and service providers.

Capacity-building efforts should pay particular attention to interoperability guidelines. For example, many guides currently exist for law enforcement agencies making requests of one State or another. However, in the future, there will be a need to develop guidelines for law enforcement agents making a request under one of several overlapping regimes, as well as guidance for the different types of data requested, depending on the nature of the data and where it is held. An appropriate tool could easily be developed. For example: imagine if an investigator were able to go to a webtool and enter in the kind of evidence sought (e.g., traffic data), from what service provider, and where that service provider is located (which State). That tool might tell an investigator in State A that the data sought could be compelled from State B and could also advise the investigator as to the appropriate legal process required. The CTED/UNODC Global Initiative will increasingly focus on this challenge, having already developed standardized forms for requesting data abroad.

Regional and cross-regional partnerships might be a particularly useful avenue for pursuing capacity-building. For reasons that are both obvious and quite technical, many cross-border requests for data actually occur within the same region, with many being concentrated in just a few States. For example: law enforcement agents are very often focused on criminal activity within a particular multi-State region where there is shared commerce, movement of peoples, and perhaps a shared language. For technical reasons, service providers might not store all their users' data in every State but will very often store it in a datacentre that is in the same region, thus ensuring that the data travels a relatively short distance to users in that region. This means that regional capacity-building efforts might make increasing sense and that cross-regional partnerships might also be useful.

It is necessary that international human rights law be a central component of all capacity-building programmes, in accordance with the relevant Security Council resolutions. It is imperative that the protection and respect of the right to privacy and data protection, in particular, be upheld by ensuring that personal data is collected, stored, processed, used, transferred and disclosed in a manner that protects individual's privacy. The United Nations Human Rights Committee (HRC) has also underlined a number of human rights considerations and safeguards relating to data retention, sharing, and privacy when reviewing the implementation by States parties of the ICCPR. These should be taken

under consideration for reforms and in the design and delivery of capacity-building efforts.[71, 72]

Capacity-building efforts can and should also focus on the private sector. As noted above, smaller service providers may simply lack the necessary resources or tools to manage law enforcement requests from around the world. Larger firms could be enlisted to help smaller firms, not with handling individual requests but rather with training materials and tools for managing incoming law enforcement requests. Moreover, NGOs and industry groups could engage with relevant stakeholders to ensure that capacity is uniform and adequate among both larger and smaller service providers. Dialogue and training between service providers, law enforcement authorities, and civil society groups could be especially fruitful.

There are many useful examples of this kind of private sector capacity-building. One notable example is the Global Internet Forum to Counter Terrorism (GIFCT),[73] which was formed in 2017 with funding from Microsoft, Twitter, Facebook, and YouTube. The GIFCT has provided a forum for regular information sharing across firms, developing technological solutions for the responsible management of violent extremist content, and developing industry best practices. Similarly, Tech Against Terrorism (an initiative initially launched by CTED) works with "big tech" and the GIFCT to support smaller platforms to prevent abuse of their platforms by terrorist actors.

IV. CONCLUSION

The state of law enforcement access to cross-border data is currently in considerable flux. Fortunately, there are several significant and consequential reform efforts under way that could constitute major milestones in the resolution of cross-border cybercrime and cooperation on digital evidence and contribute to global efforts to coordinate global law enforcement requests for access to electronic evidence. However, until they are finalized,

---

[71] As cited in the CTED-UNODC-IAP *Practical Guide for Requesting Electronic Evidence Across Borders*, page 27: Ensure that national legislation is harmonized with ICCPR, article 17, notably, legislation enshrining blanket data retention regimes for all telecommunication service providers or wide scope extended police powers; Ensure that any interference with the right to privacy, with the family, with the home or with correspondence is authorized by laws that are publicly accessible; contain provisions that ensure that collection of, access to, and use of communications data are tailored to specific legitimate aims; are sufficiently precise and specify in detail the precise circumstances and procedures for the use and storage of data collected; Adequate safeguards against unnecessary and disproportionate interference with privacy of individuals in the context of online interception and surveillance, including data mining and large-scale interception of bulk telecommunications data, hacking and file decryption by the State security and intelligence services; Institutional safeguards that spell out the conditions under which, if at all, data can be shared with foreign intelligence services, including independent oversight mechanisms and judicial involvement in the authorization of such measures; Effective safeguards to the right of defense, including, if applicable, the opportunity to investigate and challenge the reliability of electronic data use as a source of evidence in a criminal case; Procedural safeguards to notify victims whose right to privacy has been infringed through State-authorized surveillance activities about the infringement and provide them with an effective remedy in case of abuse; Safeguards put in place against unwarranted and excessive interference with the right to privacy as well as steps taken to increase the transparency of surveillance systems.

[72] For more information, see the following HRC documents available at: https://uhri.ohchr.org/en/search-human-rights-recommendations CCPR/C/EST/CO/4 (CCPR 2019), CCPR/C/EST/CO/4 (CCPR 2019), CCPR/C/NOR/CO/7 (CCPR 2018), CCPR/C/PAK/CO/1 (CCPR 2017), CCPR/C/CHE/CO/4 (CCPR 2017), CCPR/C/ZAF/CO/1 (CCPR 2016), CCPR/C/GBR/CO/7 (CCPR 2015), CCPR/C/GBR/CO/7 (CCPR 2015), CCPR/C/GBR/CO/7 (CCPR 2015).

[73] www.gifct.org.

it is difficult to know which aspects of the various challenges will be resolved and which aspects will persist. As with any reform effort, of course, there is also the possibility that unanticipated problems will arise.

At a minimum, the existence of several competing and overlapping reform efforts raises the prospect of a fragmented landscape in which investigators in some States have access that investigators in other States do not, and vice-versa. Moreover, the creation of "access clubs" raises the challenge of interoperability.

Amid these ongoing reform efforts, it will be necessary to identify ways to ensure that reform efforts can co-exist without recreating the coordination problems already faced by investigators and to develop tools and training materials to expand capacity as investigators navigate a fragmented cross-border legal landscape.

Moreover, as interoperability and capacity issues are addressed, simultaneous efforts will need to be made to ensure universal acceptance of the resulting reforms, including through ensuring respect for human rights and fundamental freedoms. It is essential that a broad range of stakeholders – including civil society, academia, and the private sector – provide input for their development in order to ensure they are drafted in a comprehensive and holistic manner, with adequate civil and human rights protections, so that they are ultimately implemented in accordance with a whole-of-society approach.