Advanced Sciences and Technologies for Security Applications

Hamid Jahankhani
Babak Akhgar
Peter Cochrane
Mohammad Dastbaz *Editors*

Policing in the Era of AI and Smart Societies

Springer

Advanced Sciences and Technologies for Security Applications

Indexed by SCOPUS

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Hamid Jahankhani · Babak Akhgar ·
Peter Cochrane · Mohammad Dastbaz
Editors

Policing in the Era of AI and Smart Societies

Springer

Editors
Hamid Jahankhani
International Journal of Electronic Security and Digital Forensics, London Campus
Northumbria University
London, UK

Peter Cochrane
Cochrane Associates Limited
University of Suffolk
Ipswich, Suffolk, UK

Babak Akhgar
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research
Sheffield Hallam University, CENTRIC
Sheffield, South Yorkshire, UK

Mohammad Dastbaz
Waterfront Building
University of Suffolk
Ipswich, Suffolk, UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-030-50612-4 ISBN 978-3-030-50613-1 (eBook)
https://doi.org/10.1007/978-3-030-50613-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Policing in the Era of AI and Smart Societies

By the beginning of 2020 the importance of AI, the Internet of Things and the cyber-spatial context of our lives already was in all our minds. Then events of the Spring of 2020 raised our consciousness to a critical level. Once the Covid-19 lockdown started, and was rolled out in almost every country, perforce we all became knowing inhabitants of the virtual world. Some, working hard from our homes, entered the world of virtual meetings several times daily, across a range of business activities, 'dinner parties', maintaining proximity to family, and entertainment. In much of this we threw caution to the winds, necessarily ignoring security to affect communicative facility. This book is timely, providing focus to our state of knowledge, and to our voluntary (if often unconsidered) sacrifice of confidentiality.

Lawyers constantly are challenged with jurisdictional problems in criminal and civil fraud cases, especially those in which the important evidence is in electronic form. The sharing of such evidence between physical jurisdictions is key to cases being investigated fully or at all, presented ethically, and justice with integrity being done. This will require growing international assent to the reality that the World is becoming a single jurisdiction for these purposes. As the second chapter of the books demonstrates, the policing of space is unable to be controlled by any single jurisdiction or any national interpretation of the Rule of Law. The challenges to finding and assembling evidence in such cases are illustrated by the statistical certainty that by 2025 there will be over 20 billion devices connected to the Internet, each a potential repository for evidence, an invisible needle in a cosmic haystack.

Policing must evolve as quickly as AI. The book argues for the urgent need to develop and adopt proactive and preventive techniques to identify and curb cyber and cyber-enabled crimes. This will need to be done on a fully international basis, if necessary labelling pariah states which choose not to cooperate.

An interesting case is made for the use of blockchain to ensure lawfulness, transparency and governance of organ supply. It is well known that unethical organ supply occurs, sometimes taking cruel advantage of deprived communities. Sophisticated technology would make it much easier to ensure that ethical principles self-evidently applicable to organ transplantation would be followed. This subject is complicated by challenges posed by data protection compliance, but the book rises to meet such challenges in an informed and creative way.

Chapter "Algorithms Can Predict Domestic Abuse, But Should We Let Them?" tackles the issue of the use of algorithms as a predictor of domestic abuse, physical and sexual. Is this a legitimate policing tool? Can we justify the use of the Internet of Things in this context? In many a 'smart home' there are devices which could provide key evidence? How do we reconcile the use of investigatory powers through devices, against the imperative of proportionate privacy for all citizens?

The following chapter addresses control of 'sexting', balancing risk against potentially heavy-handed use of the criminal law against what in some cases might be seen as non-abusive image sharing by young people with equivalent decision-making capacity. The public interest issues encountered in these chapters will test ethicists and computer scientists in the future.

Also much discussed today, and covered fully in the book, are issues of predictive policing through the use of AI. Described as the potential 'ace card' that outstrips and eclipses human minds, AI is capable of digesting vast quantities of data and recognising patterns that escape mere humans. This raises important questions about the structure, powers and accountability of information gatherers, of the technology they use and the consequent changes in society.

All generations have faced quantum challenges of this kind. For example, generations of scepticism delayed the large-scale construction of drains in London until, after the Great Stink of 1858, Parliament realised the urgency of the problem and resolved to create a modern sewerage system. That was a merely local challenge. The legal, political and philosophical matters raised in this excellent book face the whole World, and much is to be learned from the chapters that follow.

April 2020

Lord Alex Carlile
Berriew CBE QC
London, UK

Contents

Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters

Oriola Sallavaci

Abstract This chapter analyses the recently proposed EU legal framework on cross-border access to e-evidence for criminal justice purposes. The analysis is placed within the broader context of transformations that the use of technology brings not only on the socio-economic aspects of life but also the increasing challenges posed for the criminal justice in dealing with new forms of crime and globalisation of evidence. This study aims to contribute to the ongoing debate through an analysis of the specific provisions of the E-evidence framework, recommending amendments that would help achieve a balanced approach between efficient criminal investigations and the protection of fundamental rights. At the same time this study addresses what has not received sufficient attention: the challenges posed to traditional principles of cross-border cooperation in the EU and beyond, mutual recognition and mutual trust, the concept of jurisdiction and territoriality, dual criminality, the concept of privacy in the digital age, personal data protection and procedural rights of suspects in criminal proceedings. Through the lens of E-evidence this chapter aims to reflect on these challenges and offer new perspectives.

Keywords Electronic evidence · Cross border access · Data protection · Criminal proceedings · European production order · European preservation order · CLOUD Act

List of Abbreviations

AFSJ	Area of Freedom, Security and Justice
Art.	Article/Articles
CCC	Convention on Cybercrime
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union

O. Sallavaci (✉)
University of Essex, Colchester, UK
e-mail: O.Sallavaci@essex.ac.uk

H. Jahankhani et al. (eds.), *Policing in the Era of AI and Smart Societies*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-50613-1_1

GDPR	General Data Protection Regulation
ECHR	European Convention on Human Rights
EIO	European Investigation Order
EPOC	European Production Order (Certificate)
EPOC-PR	European Preservation Order (Certificate)
EU	European Union
JHA	Justice and Home Affairs
LEA/LEAs	Law Enforcement Authority/Authorities
MLA	Mutual Legal Assistance
MS/MSs	Member State/Member States
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
US	United States of America

1 Introduction: The Changing Nature of Crime and Evidence in Cyberspace

The remarkable developments in computing and information technology in the past decades have transformed every aspect of life. Cyberspace has become an essential element of modern life, crucial to our economies and societies. The growing use of social media, webmail, messaging services and applications to obtain information, communicate, work and socialise result in ever rising data flows across borders. Alongside undeniable benefits, this new reality provides the environment for misuse and abuse, facilitating new forms of criminal activities which did not exist few decades ago. Examples include the spread of viruses and other malicious software, hacking, distributed denial of service (DDoS) attacks and ransomware.[1] At the same time, the use of information and communication technologies (hereafter ICT) has transformed the very nature of some 'traditional' types of crime in terms of the way they are committed, their scale and reach affecting many aspects of life from financial transactions and commercial activities to public security—facilitating disorder, harassment, threatening behaviour and sexual offending among others.[2]

The use of technology has transformed many crimes into crime without borders. The borderless nature of cyberspace, the sophistication of the technologies and offenders' *modi operandi* pose specific and novel challenges for crime investigation and prosecution which in practice may lead to impunity. Cybercrime, in whatever

[1] These are referred to as cyber dependant crimes, also known as computer related crimes. These are offences that can only be committed by using a computer, computer networks, or other forms of information and communications technology (ICT). See Home Office (2013) *Cybercrime: A review of the evidence* Research Report 75, ISBN 978 1 78246 245 3, p. 4 available at https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence.

[2] Cyber-enabled crimes are traditional crimes facilitated by the use of ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. Ibid.

form that it takes, can instantaneously be committed across national borders. Victims of crime can be situated miles away from the offender. Offenders can easily manipulate and hide their location as well as their identity. From a practical perspective, even where authorities manage to identify a suspect, it is challenging to attribute the use of an electronic device to that particular individual i.e. to identify the person behind a screen or keyboard or establish a connection between a computing device and a particular individual.

For all Cybercrime, data remains the key element, both from a crime perspective and from an investigative perspective. Whereas criminals require and target data for most of their crimes, law enforcement agencies (hereafter LEA(s)) need access to relevant data for their investigations. Electronic information (hereafter e-information) can be used for intelligence purposes and crime prevention, to combat ongoing crime by disrupting online criminal activities (e.g. by bringing down websites) and for evidential purposes in criminal proceedings. Electronic evidence (hereafter e-evidence) is paramount for all types of crime that can leave a digital trace, even if that is only some form of electronic communication. These could include serious crimes such as terrorism, child sexual abuse, human trafficking and the like, as well as lower impact, high volume crimes such as spread of malicious software (such as ransomware, spyware etc.).

An increasing number of criminal investigations rely on e-evidence and this goes beyond cyber dependent and cyber enabled crimes. From an evidential point of view, today almost every crime could have an e-evidence element as often offenders use technology, such as personal computers, notepads, camera phones, where they can leave traces of their criminal activity, communications or other information that can be used to determine their whereabouts, plans or connection to a particular criminal activity. E-evidence could include different types of data such as messages exchanged via various social-media applications, information on the holder of email accounts or the content of those emails, information on the timing of online calls via Skype, Viber, WhatsApp etc. These types of data have different levels of relevance in the context of criminal proceedings: subscriber data could be useful in obtaining the identity of a suspect; access logs could be useful in connecting a suspect user to a particular action; metadata and content data can be most relevant as probatory material.[3]

There are several closely linked characteristics of e-evidence that pose particular challenges for crime investigation. First, e-evidence is volatile and can be transmitted, altered or deleted easily. For this reason, effective and timely access by public authorities is vital to enable the investigation and prosecution of crime. External factors such as specific legal requirements contribute to the volatility of e-evidence, increasing challenges for investigations and prosecutions. Examples are (a) the lack of mandatory data retention rules[4] and (b) data minimisation requirements that force service

[3] See below the discussion of different type of data. See European Commission (2018) "Commission Staff Working Impact Assessment" p. 13. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN.

[4] For instance there are no mandatory data retention rules in the US (which is of importance given that the key SPs operating in the EU are US based) nor in the EU, since The Data Retention Directive

providers (hereafter SPs) to delete data more quickly.[5] Two closely linked problems to volatility of e-evidence, posing challenges for LEAs, concern the availability and location of electronic data. Often data are available only to private infrastructures which may not be located in the same country as the investigating authorities and are therefore subject to different jurisdictions imposing different rights and obligations. Even where the information is publicly available, it might move into systems that require special credentials to access. As a result LEAs require the cooperation of these private infrastructures or other LEAs situated in different countries from where the investigation is taking place.[6]

In addition to the above, determining the location of data may be difficult. Data can be split between different countries and can be copied in multiple countries. It can be moved quickly and effortlessly. Data stored in the cloud are mirrored for security and availability reasons, and can therefore be found in multiple locations within a country or in several separate countries. Data are thus located in different jurisdictions at the same time. Due to this and to cached versions of data, not even the SPs might know where the sought-after data are exactly located. The challenge posed by data moving swiftly across jurisdictions is a consequence of internet governance and the business models of the SPs that have evolved over the past decades across the world.[7]

This state of affairs is referred to as "globalisation of criminal evidence".[8] Crime today often has a cyber component and with it an increasingly prominent cross border dimension. Even crimes that may appear not to have a cross border dimension can actually have one because of e-evidence. In 2018 the European Commission found that in the EU "more than half of all investigations involve a cross-border request to access [electronic] evidence."[9] Yet alarmingly "almost two thirds of crimes involving

2006/24/EC was declared invalid by CJEU in case C-293/12 *Digital Rights Ireland Ltd v Minister of Communications* ECLI:EU:C:2014:238.

[5] Data minimisation is enshrined in the General Data Protection Regulation (GDPR): The processing of personal data must be adequate, relevant and limited to what is necessary—Article 5(1)(c). Data minimisation requirements force service providers to delete data more quickly, increasing the number of cases where data will no longer be available when LEA's request reaches the service provider.

[6] This problem is well recognised. See for instance Eurojust and Europol (2019) *Common challenges in combating Cybercrime* Joint Report, available at https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime See also European Commission (2018) "Commission Staff Working Impact Assessment" p. 19.

[7] European Commission (2018) "Commission Staff Working Impact Assessment" p. 13.

[8] Ibid p. 35.

[9] Ibid p. 14 See also data, albeit partial, on crimes that cannot be effectively investigated or prosecuted. The same report also found that "Less than half of all the requests to service providers are fulfilled" p. 15 According to the Commission a request could remain unfulfilled for several reasons, including that the request is sent to a provider who does not hold the data, it is excessively broad or unclear, it fails to specify an (existing) account or sought information, it does not have a valid legal basis or the data sought no longer exists—p. 17.

cross-border access to e-evidence cannot be effectively investigated or prosecuted".[10] The ability of LEAs to access the data needed to conduct criminal investigations is an increasing challenge.[11] This is partly due to technological developments, such as the enhanced use of encryption and other techniques which criminals abuse to obfuscate their tracks, as well as cryptocurrencies to hide their illicit earnings. However, the lack of accessibility to relevant data also comes due to legislative barriers or shortcomings that must be overcome to enhance cross-border access to electronic evidence and the effectiveness of public-private cooperation through facilitated information exchange. These barriers are often related to the principle of territoriality, which sets limits to the scope of jurisdiction and to the investigative powers which law enforcement and judiciary have at their disposal under their national law. As a result, the tools in the hands of LEAs do not provide what is necessary to deal with data flows, for which questions of territoriality are of no relevance as Cybercrime does not recognise borders and e-evidence has become increasingly global.

Improving access to electronic information for law enforcement and intelligence purposes is therefore a pressing issue concerning almost every type of crime. Countries around the world are responding with new legal frameworks and instruments, changes to law enforcement procedures and governance of the internet. The approaches currently taken in an international level span from a government controlled internet characterised by data nationalism and localisation often justified in the name of security, usually resulting in a censored or unfree cyberspace on the one extreme,[12] to a global internet driven by a multi-stakeholder governance model, characterised by free flow of data, which emphases transnational cooperation for the purposes of data access, on the other end of the spectrum.[13] A majority of countries referred to as 'digital deciders' stand somewhere in between and could gravitate toward either end of the spectrum whilst also supporting a third approach that manifests elements of the two extremes.[14] While the global cyber reality is constantly changing and shifting between these two poles, the legislative changes adopted by many countries have consequential effects on the efficiency of criminal investigations and prosecutions as well as on fundamental rights of individuals, including the right to privacy and data protection.

---

[10] Ibid at p. 17 This is partly due to lack of timely access i.e. leads disappear or lack of access i.e. access denied.

[11] See Eurojust and Europol (2019) *Common challenges in combating Cybercrime* Joint Report.

[12] Data nationalism refers to measures taken by some countries to require that data be stored, processed, or handled within their borders in an attempt (or rather justification) to protect privacy and security and to promote economic growth. Russia, China, India and other countries, have enacted laws that require such *data localization*. https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures7-29-2016.pdf.

[13] Robert Morgus, Jocelyn Woolbright, & Justin Sherman The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet, October 2018, available at https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

[14] Ibid. Every jurisdiction has sought to exercise certain degree of control from the early days of the internet, see e.g. Lessig and Resnick [38] 'Zoning speech on the internet: a legal and technical model' *Michigan Law Review*, Vol. 98, No. 2 (Nov., 1999), pp. 395–431.

This study focuses on an important and recent legislative initiative: the EU legal framework on cross-border access to e-evidence for criminal justice purposes. The important legislative package referred to as "E-evidence", aimed at facilitating the access to e-evidence by European LEAs, contains two texts: a draft Regulation[15] providing two new mechanisms for LEA's cross border access to e-evidence (European Production Order (EPOC) and European Preservation Order (EPOC-PR)) and a draft Directive[16] which requires every online service provider (hereafter SP) "established" in or that has "substantial connection" to at least one EU Member State (hereafter MS) to appoint a legal representative in the territory of an EU MS of choice as an addressee for the execution of the above Orders. While both the texts will be discussed, the following analysis shall be based heavily on the draft Regulation.

The proposed legal framework was introduced by the EU Commission in April 2018. On 7 December 2018 the Council adopted its own draft[17] (known as Council's "general approach") which was forwarded to the EU Parliament. The EU Parliament is yet to adopt its position[18] before the 'trilogue' procedures amid the EU Parliament, the Council and the Commission can start in order to agree to a common text.[19] Given that the E-evidence framework is currently being negotiated, the following analysis and findings aim to contribute to achieving the best version of the forthcoming instruments. This study is based on the legal provisions currently contained in the Commission's proposal, the Council's draft and the recently published draft report of the LIBE's rapporteur Birgit Sippel, to be presented to the EU Parliament in 2020,[20] which at the time of writing, is yet to receive academic attention.

---

[15]European Commission "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters" Strasbourg, 17.4.2018 COM (2018) 225 final, 2018/0108(COD) available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

[16]European Commission "Proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" Strasbourg, 17.4.2018, COM(2018) 226 final, 2018/0107(COD) available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

[17]Council of the EU "Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters—general approach" (10206/19) Brussels, 11 June 2019 available at https://data.consilium.europa.eu/doc/document/ST-10206-2019-INIT/en/pdf.

[18]During 2018–2019 EU Parliament has been advancing very slowly. E-evidence has been assigned to the LIBE Committee. Partly due to the European 2019 elections, LIBE is still to adopt its report, which would then be submitted to the Plenary of the Parliament for adoption.

[19]It is expected that the framework will be approved by 2020 and will come into force in 2022.

[20]European Parliament "DRAFT REPORT on the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM(2018)0225—C8-0155/2018—2018/0108(COD))" Committee on Civil Liberties, Justice and Home Affairs, November 2019, Rapporteur: Birgit Sippel Available at https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf.

The following analysis of the E-evidence framework is placed within the broader context of transformations and challenges posed by the use of technology for the criminal justice in dealing with cross border crime and globalisation of evidence. This study aims to contribute to the current debate in what is mainly practice/practitioner oriented literature[21] through an analysis of specific provisions of the framework itself and by proposing improvements to the draft instruments through a set of recommendations. At the same time, this study addresses what has not received sufficient attention in the academic literature: the challenges E-evidence poses for, and the perspectives it opens up in relation to traditional principles of cross-border cooperation in the EU and beyond such as mutual recognition and mutual trust, the concept of jurisdiction and territoriality, personal data protection and the concept of privacy in the digital age as well as dual criminality, equality of arms and procedural rights of the suspects. Building on existing literature[22] it demonstrates how these principles are being challenged and developed in the context of E-evidence.

The EU E-evidence framework is of particular importance in shaping the future of similar instruments and the terms of cooperation between countries all over the world. This study explores the framework's position with regard to specific aspects of the US CLOUD Act 2018[23] which in itself marks a major change in how cross-border access to e-evidence may develop in the rest of the world. At the time of writing, the US has just negotiated the first CLOUD Act executive agreement with

[21] See European Data Protection Board (EDPB) (2018) "Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters" available at https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf; European Data Protection Supervisor (EDPS) (2019) "EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters" Opinion 7/2019, November 2019 available at https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf; European Criminal Bar Association ECBA (2019) ECBA Opinion on the European Commission's Proposals, available at http://www.ecba.org/extdocserv/20190213-ECBAonEPOsEPROs_Final.pdf; Statement of Article 29 Working Party (2017) "Data protection and privacy aspects of cross-border access to electronic evidence" Brussels 29 November 2017 available at https://www.hldataprotection.com/files/2018/02/20171129-Art.-29-WP-e-Evidence_Statement.pdf; The Council of Bars and Law Societies of Europe (CCBE) (2019) CCBE recommendations on the establishment of international rules for cross-border access to electronic evidence 28/02/2019; The Council of Bars and Law Societies of Europe (CCBE) (2018) CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters 19/10/2018; Theodore Christakis (2019) "E-evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead" Cross-border Data Forum available at https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/.

[22] See inter alia V. Mitsilegas (2016) EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe, Oxford/Portland: Hart Publishing; S. Peers (2016) EU Justice and Home Affairs Law, Vol II. Oxford University Press; Bermann PS (2018) "Legal Jurisdiction and the Deterritorialization of Data" Vanderbilt Law Review, Vol. 71: 11; J. Daskal (2015) "The Un-Territoriality of Data" Yale Law Journal, Vol. 125 (2), 326; C. Janssens (2013) The principle of Mutual Recognition in EU Law, Oxford University Press;.

[23] Clarifying Lawful Overseas Use of Data Act—CLOUD Act provides the legal basis for the United States government to conclude agreements with foreign governments on access to data held by United States service providers and vice-versa.

the United Kingdom[24] which is to be followed by another one with Canada.[25] The EU E-evidence framework shall influence and at the same time needs to conform to a number of new agreements currently being negotiated. In 2019 the EU Commission received negotiating mandate to achieve an agreement between the EU and US[26] as well as to shape the second amending protocol of the Cybercrime Convention (hereafter CCC).[27] Both these instruments need be negotiated from the perspective of the forthcoming provisions of the E-evidence framework therefore it is important that the latter offers provisions that increase the efficiency of investigations and prosecutions by surpassing challenges in cross border cooperation, while maintaining safeguards to fundamental rights of individuals.[28] This study aims to contribute in achieving this objective especially given that, in the global arena, E-evidence framework represents the model to be followed by countries that have embraced or are willing to adopt a free internet governance model as noted above. This is particularly important in the context of recent counter developments taking place in the United Nations General Assembly which seem to favour a state control over the internet and data nationalism model.[29]

---

[24] Available at https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019?utm_source=b4d391f0-3d36-4077-8793-d5b2b06944c1&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate.

[25] The Canadian Association of Chiefs of Police has passed a resolution calling for negotiation of an executive agreement with the U.S. under the CLOUD Act. See https://www.cacp.ca/resolution.html?asst_id=1694.

[26] Council of the EU "Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters" (9114/19) Brussels, 21 May 2019, available at https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf.

[27] Council of the EU "Decision authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime" (CETS No. 185) Brussels, 21 May 2019 available at https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf In June 2017, the 61 parties to the Budapest Convention on Cybercrime agreed to launch the preparation of an additional Second Protocol to the Convention to help law enforcement secure evidence on servicers in foreign, multiple or unknown jurisdictions. This Second Protocol is expected to be agreed by the end of 2020. See Council of Europe (2019) available at https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07.

[28] As noted by the Cybercrime Convention Committee (T-CY) "close coordination in the drafting of the Additional Protocol to the Budapest Convention and the preparation of relevant legal instruments by the European Union should be pursued". Ibid.

[29] On 18 November 2019, the Third Committee of the United Nations General Assembly adopted the resolution "Countering the use of information and communications technologies for criminal purposes" favouring a state control over the internet and data nationalism model. The resolution was backed by Russia and sponsored by a coalition of 45 countries including China, Cuba, North Korea, Nicaragua, Syria, Venezuela, and passed 88–58 with 34 abstentions. It is reported that a committee of experts will meet to draft the treaty in August 2020. Ahead of the adoption, a coalition of countries with the United States in the lead encouraged opposition to the resolution with the argument that it would increase state-backed control over the internet. It was also reported that Russia has presented the resolution as an alternative to the Budapest Convention, ratified

While the future remains uncertain, this study posits that the globalization of criminal e-evidence is driving historic change in the rules as to how LEAs can gain access to communications and other electronic information which has to be consistent with privacy and human rights protection standards. Through the lens of the E-evidence framework, this study throws light on the challenges and transformations that lie ahead of relevant aspects of EU criminal law. These challenges and transformations are often perceived as a weakening of the safeguards and threats to traditional methods of cooperation.[30] This study argues that in order to deal adequately with these challenges, new legal instruments such as E-evidence are required to offer the mechanisms necessary to facilitate the investigation and prosecution of crime while at the same time providing safeguards and guarantees that the rights and interests involved will be adequately protected. While these may manifest as competing objectives, in fact they serve a common purpose, for the public interest is equally invested in efficiently combating crime *and* protection of fundamental rights. Tensions that arise in the balancing process need be addressed by imaginative and forward thinking measures. It is not possible to move forward by resisting challenges and change, by hanging on to outdated mechanisms that ought to evolve, or by aiming to achieve something new whilst not changing anything of essence in the process.

This study is presented in two parts. By analysing the status quo, the first part explores the position that the proposed legal framework takes within the existing instruments for cross border access to e-evidence within the EU and beyond. It explores its impact in the development of the concept of territorial jurisdiction, sovereignty and the principle of mutual recognition. The second part takes a closer look at the provisions of the framework and the proposed instruments from a safeguards perspective. The detailed analysis of the Commission's proposal, Council's draft and the LIBE's rapporteur draft report for the EU Parliament informs this study's recommendations for a balanced and principled approach to cross-border e-evidence access and efficient prosecutions, whilst maintaining respect for fundamental rights and affected states' interests.

in 2001 by 64 member states but which has never been adopted by Russia. For a critique see the US position available at https://usun.usmission.gov/statement-on-agenda-item-107-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes/.

[30] See for instance The Council of Bars and Law Societies of Europe (CCBE) (2019) CCBE recommendations on the establishment of international rules for cross-border access to electronic evidence 28/02/2019; The Council of Bars and Law Societies of Europe (CCBE) (2018) CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters 19/10/2018.

2 Part 1: The E-evidence Framework: A New Paradigm of Transnational Cooperation in Criminal Matters

2.1 From Mutual Legal Assistance Requests to Extraterritorial Unilateral Orders: An Organic and Necessary Development?

Transnational cooperation in criminal matters, including cross border access to evidence located outside the jurisdiction of the investigating or prosecuting authority, has traditionally been regulated via international agreements establishing respective terms and conditions for Mutual Legal Assistance (hereafter MLA). MLA entails the formal cooperation between the competent authorities of different countries on a *request* to collect and transfer the evidence from the country where the evidence is located to the requesting state. MLA agreements are a cornerstone of global cooperation on law enforcement and one of the most widely used mechanisms for requesting foreign assistance in domestic criminal investigations and prosecutions.[31] However, MLA agreements have struggled to keep pace with the changing nature of crime and evidence, especially considering the globalization of data. At the same time the number of MLA requests has increased significantly and the matters involved have grown increasingly more complex. MLA requests take too long to process (from 1 to 18 months), there are no fixed deadlines for responding and the mechanism is complex and diverse from country to country.[32]

Figure 1 illustrates the stages and actors involved in the traditional MLA process. On the one hand, the formal procedures and multiple authorities involved act as safeguards for the protection of individual rights and national interests, yet at the same time they contribute to significant delays and the recognized inefficiency surrounding the MLA system which is problematic especially considering the volatility of E-evidence.[33] The admissibility and execution of MLA requests is subject to the receiving country's national legislation which may result in a refusal of the MLA request on various grounds such as the difficulty to establish a probable cause, lack

[31] The MLA treaties are generally broadly worded to allow for cooperation on a wide range of law enforcement issues including locating and extraditing individuals, freezing assets, requesting searches and seizures etc. They are a necessary tool in combating transnational crime such as money laundering and human trafficking and in prosecuting criminals who attempt to evade domestic law enforcement by operating abroad. See for example the European Convention on Mutual Assistance in Criminal Matters For an account see Steve Peers (2016) EU Justice and Home Affairs Law, Vol II. Oxford University Press.

[32] See Council of EU Non Paper (15072/16) available at http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf.

[33] Ibid para 2.2.1 See also Council of Europe T-CY report (2013) available at https://rm.coe.int/16802e726c.

Fig. 1 MLA process
Source European Commission "Security Union: Facilitating Access to Electronic Evidence" Factsheet, April 2018 available at https://ec.europa.eu/info/sites/info/files/placeholder_2.pdf

of dual criminality, data not available due to deletion, incomplete or inadequate requests.[34]

The general framework established by MLA treaties[35] has been further developed by the Council of Europe Convention on Cybercrime (CCC)[36] that entails specific rules for access to e-evidence. These include inter alia: the expedited preservation of stored computer data (Art. 16 CCC); the expedited preservation and partial disclosure of traffic data (Art. 17 CCC); production orders (Art. 18 CCC).[37] In order to address the deficiencies and the ambiguities of the treaty framework, the Cybercrime Committee is working on a second additional protocol to the CCC which shall provide for more effective MLA proceedings, rules allowing for direct cooperation with service providers in other jurisdictions, a clearer framework and stronger safeguards, including data protection requirements for existing mechanisms of cross-border access to computer data. It is expected that the draft protocol shall be finalised by the end of 2020.[38]

---

[34]Council of EU Non Paper (15072/16) available at http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf.

[35]Such as European Convention on Mutual Assistance in Criminal Matters of 20 April 1959.

[36]Council of Europe Convention on Cybercrime of 23 November 2001. To date the Cybercrime Convention has been ratified by most EU MSs (except for Ireland and Sweden) and several non-European countries including the US. See the chart of signatures and ratifications https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=w8r6xLCC.

[37]The list of measures covers not only investigative powers (Art. 18 ff. CCC), but also provisional measures aimed at the preservation of electronic evidence (Art. 16, 17 CCC). The powers are subject to conditions and safeguards that seek to balance the requirements of law enforcement with the protection of human rights (Art. 15(1) CCC) and include both procedural (judicial or other independent supervision) and substantial (proportionality, limitation of certain measures to serious offences) requirements in accordance with the principles of the respective national criminal justice system (Art. 15(2) CCC).

[38]Cybercrime Convention Committee (T-CY), Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3, p. 3 available at https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07.

Within the EU, the traditional MLA framework for cross border access to evidence has been replaced by the European Investigation Order (EIO)[39] which provides for the gathering and transfer of evidence between MSs, based on the principle of *mutual recognition* (Art. 67(3), 82(1) TFEU). EIO replaces the traditional framework of MLA proceedings based on a *request* by a system of transnational judicial cooperation between the MS that issues the EI *order* (the issuing MS, formerly the requesting state) and the MS that recognises and executes the EIO (the executing MS, formerly the requested state). Similarly to MLA, the EIO mechanism entails a formal cooperation between investigative and judicial authorities of different MSs. A key difference is that the mechanism is triggered by an *order* issued by the requesting MS rather than a *request* as is the case with MLA agreements. The EIO mechanism still requires a decision of another MS to recognise and execute the production order, which is done under the same conditions as if the investigative measure had been ordered by an authority of the executing MS (Art. 9(1) EIO Directive). In this regard, several traditional obstacles to MLA haven been abolished (such as the exceptions for political and fiscal offences). Nevertheless, the obligation to recognise and execute the EIO is still subject to a number of grounds for refusal (Art. 11(1) EIO Directive).

The scope of the EIO covers any investigative measure aimed at gathering evidence, including electronic evidence (Art. 3 EIO Directive). An EIO may only be issued if it is in conformity with the proportionality principle and the investigative measure could have been ordered in a similar domestic case (Art. 6(1) EIO Directive). Furthermore, the EIO must be issued or validated by a judicial authority (judge, court, investigating judge, public prosecutor, Art. 2(c) EIO Directive). EIO has significantly facilitated cross-border cooperation by streamlining the procedure and reducing cooperation obstacles. The EIO Directive provides for deadlines of 120 days (30 days for the executing authority to make a decision on the recognition or execution of the EIO and 90 days to carry out the investigative measure),[40] which is faster than the MLA procedure. This improvement in deadlines is still considered insufficient for accessing e-evidence in criminal investigations, for which the EIO process would still be too long and therefore ineffective.[41]

Due to the limitations and inefficiencies of the judicial cooperation channels, MSs regularly obtain *non-content data* through *direct cooperation with service providers*

[39] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, O.J. L 130/1.

[40] See article 12 of EIO Directive for time limits.

[41] See EU Commission (2018) "Impact Assessment" p. 24. Even though the EIO Directive allows for shorter time-limits where necessary "due to procedural deadlines, the seriousness of the offence or other particularly urgent circumstances" (Art. 12(2)) and article 32(2) provides for a 24 h deadline to decide on provisional measures, arguably these shorter deadlines cannot address the specific needs of e-Evidence: the first is an exception rather than the general rule, requiring reasons for urgency in every case, and the second is specifically aimed at preservation of the data only which in itself is insufficient as timely access need be provided not only preservation of data.

(SPs) on a *voluntary*[42] basis. In direct cooperation situations, the public authorities of country A directly contact the SP established in country B via production orders/requests pursuant to their national rules of criminal procedure, to request information to which the SP has access. According to CCC, a state party may unilaterally and directly access computer data stored abroad if this data is publicly available (Art. 32(a)) or if the data is accessed or received through a computer system in its territory, but located in another state party and if the accessing State Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system (Art. 32(b)). The latter provision is considered to provide a legal basis for non-mandatory production requests to foreign SPs established in another State Party.

According to the European Commission, direct cooperation with SPs has become the main channel for authorities to obtain non-content data, as reflected by the significant number of this type of requests.[43] However its efficiency is impeded by a number of factors especially related to existing legal frameworks. Within the EU, the Telecommunications Framework[44] prohibits national telecommunications providers from responding directly to requests from foreign authorities. In addition, there is no legal framework allowing direct cooperation in other communication sectors. Therefore, it is rare to non-existent and mainly used in emergency situations.[45] LEA's requests for direct cooperation to US SPs operating in the EU, are typically redirected to the US, where the SP holds the data or where the management of these requests within the company takes place. Under section 2701(2) of the Electronic Communications and Privacy Act 1986 (ECPA), US based SPs are allowed to cooperate directly with European public authorities with regard to *non-content data.*[46] The cooperation is voluntary from the perspective of ECPA, even though LEAs in some MSs may be using nationally binding orders in making the request. SPs have created their own policies or decide on a case-by-case basis as to whether and how to cooperate. Reported problems in public-private cooperation between LEAs and SPs which have hampered effective investigations and prosecutions concern the lack of standardised procedures across SPs, unreliability of cooperation, unequal treatment of MSs, lack of transparency and of accountability.[47]

A third channel used by LEAs to access e-evidence, relies on mandatory instead of voluntary cooperation. Some states have established an obligation of foreign

[42] Ibid p. 26 "Voluntary" means that there is a domestic legal title which cannot be enforced directly in the recipient country. This legal instrument may be an 'order' or 'request' hence, in the absence of a clear legal framework, the distinction between voluntary and mandatory cooperation is not always easy to establish and causes disagreements between LEAs and SPs.

[43] E.g. more than 120 000 in 2016, based on the 2016 transparency reports by Google, Facebook, Microsoft, Twitter and Apple. Ibid. p. 26.

[44] On EU Communication Framework see https://ec.europa.eu/digital-single-market/en/policies/telecom-laws.

[45] See EU Commission (2018) Impact assessment.

[46] ECPA prohibits SPs to give access to content data on a voluntary basis, except in cases of emergency.

[47] EU Commission (2018) Impact assessment pp. 25–28.

SPs to disclose relevant data irrespective of the location where the data is stored or processed, and thereby extended their enforcement jurisdiction to any provider offering electronic communication services within their territory.[48] This may even extend to *direct access* to data in cases where authorities access data without the help of an intermediary, for instance following the seizure of a device or following the lawful acquisition of login information. The national law in a number of MSs empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it, or to use credentials for an account to access and search data stored under that account.[49] This direct access mechanism has become more relevant as data is regularly stored not on the local device but on servers in different locations, possibly outside of the MS concerned or even outside of the EU. The location of data or of the perpetrator may not be known to LEAs or even SPs and it may be practically impossible to determine (referred to as "loss of knowledge of location").[50] As a result, it can lead to difficulties in establishing whether such searches have a cross-border component and of the enforcing jurisdiction in cyberspace, which requires determining the competence of relevant authorities to undertake an investigative measure across the border.

The proposed E-evidence framework seeks to address the problems and obstacles to criminal investigations associated with the existing mechanisms for cross-border access to e-evidence. During the recent years there have been repeated calls for action by the EU MSs, EU Parliament and Council which have recognised the need to improve the efficiency of mutual legal assistance and judicial cooperation instruments as well as the cooperation between MSs' authorities and SPs based in non-EU countries.[51] The proposed E-evidence framework tackles three key problems identified under the current channels of cooperation that hinder effective investigations and prosecutions: 1. The impact of the current slow procedures under existing judicial cooperation channels to access e-evidence across borders, especially given its volatile nature; 2. Multiple inefficiencies in the public-private cooperation between service

[48]Eg. Art. 46 of the Belgian Code of Criminal Procedure; for the application to foreign providers see the judgment of the Hof van Cassatie [Belgian Court of Cassation], Judgment of 1 December 2015, P. 13.2082.N, Yahoo. See European Parliament Policy Department for Citizens' Rights and Constitutional Affairs (2018) Report.

[49]Member States have different approaches to direct access and the data storage location—see section 2.2.3 EU Commission (2018) Impact Statement.

[50]Ibid p. 32.

[51]See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, COM (2015) 185 final; Communication on delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, COM/2016/0230 final; Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16; Council of the EU, Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating Cybercrime", ST 12711 2017 INIT, 2 October 2017. In October 2017 the European Parliament adopted the Resolution of 3 October 2017 on the fight against Cybercrime (2017/2068(INI) calling on the Commission to put forward a European legal framework for electronic evidence.

providers and public authorities; 3. Shortcomings in defining jurisdiction, limitations in how authorities can use investigative measures in cross-border situations and lack of clear frameworks for cooperation with SPs.[52]

The proposed framework creates two new cooperation instruments, namely the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR) and provides for an obligation of SPs to designate a legal representative in the Union for the receipt of, compliance with and enforcement of the new cooperation instruments. EPOC provides a faster tool for obtaining electronic evidence with deadlines of no longer than 10 days and 6 h for emergency situations. EPOC-PR shall be used to avoid deletion of electronic evidence. Since the electronic data will no longer travel back through multiple steps and authorities but go directly from the legal representative to the authority requesting the data, the procedure will technically be faster and more efficient.[53] In addition, the use of pre-translated and standardized forms is expected to facilitate the cooperation between judicial authorities and SPs, by providing an efficient and fact transmission of e-evidence, standardized exchange of information and cost reduction.

While EIO and the MLA channels will continue to exist, the European E-evidence framework provides a fast track alternative for the specific case of e-evidence. Its material scope is limited to criminal proceedings during the pretrial and the trial phase.[54] Unlike the EIO, the E-evidence framework of cooperation is not to be engaged in proceedings on the imposition of an administrative fine.[55] Ultimately the MSs' authorities decide on whether to cooperate under MLA, EIO or under the E-evidence framework.[56]

Despite expected improvements in the efficiency of investigations and prosecutions by simplifying and speeding up the procedures, the necessity of having *a new instrument* to organize cross border access to electronic evidence has been questioned.[57] The proposed E-evidence framework is considered as adding another layer to the already complex tableau of existing, multiple channels for data access and transnational cooperation.[58] While alternative approaches have been considered and could have been taken by the Commission,[59] in this author's opinion, a specific framework dedicated to improving access to e-evidence is more suitable to help achieve that goal than amendments to existing procedures and instruments that are general in scope and do not provide for the specific e-data related challenges. Procedural

[52] EU Commission (2018) Impact study; EU Commission "Security Union: Facilitating Access to Electronic Evidence" Factsheet, April 2018 available at https://ec.europa.eu/info/sites/info/files/placeholder_2.pdf.

[53] As it will be discussed below the authorities of the host country will only be involved in cases where there are specific legal concerns or where the Order needs to be enforced.

[54] Article 3(3) draft Regulation.

[55] Article 4(b) EIO Directive.

[56] Article 23 draft Regulation.

[57] See for example EDPB Opinion 23/2018.

[58] Ibid.

[59] In response to this criticism it is worth noting that several alternatives were considered by the Commission in its Impact assessment (2018).

improvements to existing instruments are necessary, but not by themselves sufficient to overcome the difficulties present in the current channels of cooperation.

According to EDPB, an alternative option to e-evidence framework "could have been … the use of preservation orders to freeze the data for as long as a formal request based on a MLAT is issued" which would have allowed "maintaining the safeguards provided in these instruments while ensuring that the personal data sought is not deleted".[60] As discussed further below, while it is important that the E-evidence framework has adequate safeguards, the proposed alternative measure alone would not be a sufficient improvement to the current status quo. Preserving the data alone is not sufficient as LEAs also need speedy access to those data to be able to progress with the investigation. This is particularly important in the context of Cybercrime where e-evidence is in many cases the only significant lead for investigators. Timely access is important, not only in terms of data volatility which *can* in fact be addressed by the execution of preservation orders, but also for the progress of the investigations itself.

Criminal investigations have to procced step by step, identifying first leads and then following further indications provided by those leads. These steps will often necessitate repeated, iterative requests for access to electronic information across different SPs and different jurisdictions. If the first requests are fulfilled slowly, the chances to find any data in response to further requests decrease significantly.[61] Any delays enable ongoing crimes to progress with detrimental effects on the victims of crime and society as well as enabling the perpetrators to hide or change their *modi operandi*. It is therefore important that the final e-evidence framework provides not only for the preservation of data—which in itself should allow sufficient time taking into consideration that criminal investigations are generally time consuming—but also for the fast access of those data by investigative or judicial authorities. This is an aspect that the proposed framework addresses and provides for through faster mechanisms and procedures albeit not ideal ones.[62]

It has been argued that modifications and improvements to the EIO Directive should have been explored instead of introducing some aspects of the E-evidence framework.[63] The key concern for the critics' is that the existing instruments such as EIO are perceived to have more safeguards in place than the proposed E-evidence framework, such as longer deadlines for the executing authorities to assess whether the request for execution is well founded and respects all the conditions for issuing

[60] EDPB opinion 23/2018 pp. 5–6.

[61] EU Commission (2018) Impact assessment p. 20.

[62] The standard time limit for the provision of data is 10 days—which could still be long in terms of data volatility and/or the progress of investigation. Furthermore, the proposed framework does not provide for ongoing investigations and live data collection through surveillance—see the discussion further below.

[63] See Art. 37 of the EIO Directive; EDPB 23/2018 Opinion; EU Parliament, Policy Department for Citizens' Rights and Constitutional Affairs (2018) Report.

and transmitting an EIO.[64] It is important to note here that EIO is a general instrument that is used for various forms of evidence including searches, interception of telecommunications, the gathering of witnesses and experts testimony. It is difficult to reconcile in a single instrument all the specific requirements for different types of evidence and certainly, e-evidence presents specific characteristics that require to be dealt with by specific rules and time lines. Given the general nature of the EIO instrument, even if shorter deadlines were to be introduced, these may not be adequate for other types of evidence while still being too long to adequately deal with the requests for e-evidence considering the volatility of data, data minimization requirements and investigative needs. The instruments proposed by the E-evidence framework are fundamentally different from EIO, a difference that is also reflected in procedural details. It is not possible to adequately respond to novel challenges with old mechanisms embedded in lengthy procedures and bureaucratic complexities. As it will be argued further below, the answer is to provide adequate safeguards that protect the rights and interests of all stakeholders, suited to the new type of instruments created by the E-evidence framework, albeit not identical to the ones found in existing mechanisms of transnational collaboration.

2.2 A Paradigm Shift: The Extraterritoriality of the E-evidence Framework

The E-evidence model builds upon the existing models of cooperation, yet is fundamentally different. The Commission did not pursue the idea of direct cross-border access to provider data but proposed a new framework for *mandatory cross-border direct cooperation with SPs*. Unlike current MLA/EIO procedures where the judicial authorities in both issuing and executing countries are involved, the proposed e-evidence framework allows the judicial authority of the issuing MS to address directly the legal representative of the SP established in another EU country via mandatory orders to preserve and/or produce e-evidence. The enforcing MS authorities will only get involved where necessary to ensure compliance with an order by the addressee represented in its territory. The element of 'voluntary cooperation' currently present in the *direct cooperation channel* is thus replaced by a 'mandatory cooperation order' with sanctions to be imposed on the SP in case of non-compliance.[65]

There are two major characteristics of the e-evidence framework that require further attention. First, the instruments proposed by the E–evidence framework have an extraterritorial reach. This extraterritorial dimension is in itself twofold and affects the traditional concept of territorial sovereignty and jurisdiction. On the one hand, the proposed cooperation instruments will create a transnationally binding obligation

[64] According to EIO Directive, the executing authority has 30 days to take its decision on the recognition of the request and then should execute the order within 90 days see Art. 12(3) and (4) EIO Directive. See also Art. 6 EIO Directive.

[65] See recital 59 of the draft Regulation.

of its addressee within the EU that fundamentally differs from the existing mechanisms under the current legal framework of international cooperation in the Area of Freedom Security and Justice (AFSJ). On the other hand, the proposed instruments may interfere with the territorial sovereignty of a third country by extending the enforcement jurisdiction of the issuing MS to SPs established in and data located in the third country. Both aspects will be explored further below.

The second major characteristic of the proposed framework is that it applies *regardless of the location of data* including where e-evidence is stored outside the EU. The jurisdiction that must be complied with is that of the issuing country. The distinction between domestic and cross-border access is no longer based upon the place where the data is stored, but upon the MS where the SP is established or represented.[66] Consequently the proposed framework departs from the traditional rule of international cooperation that cross-border access to computer data requires consent of the state where the data is stored.[67] Jurisdiction is no longer linked to the location of data, but to the place where the addressee of the measure provides its services.[68] According to the new approach, the jurisdiction of the EU and its MSs can be established over SPs *offering their services in the Union* and this requirement is met if the SP enables other persons in (at least) one MS to use its services and has a substantial connection to this MS.[69] In this way the proposal avoids the difficulties in establishing the place where the data is actually stored and the "loss of location" problem highlighted above.

This approach is in line with recent developments in the international arena which demonstrate a departure from data location as the determining factor for establishing enforcement jurisdiction. This tendency is clearly reflected in the Cybercrime Convention Committee's guidance note on production orders and the existing laws of a number of MSs providing for cross-border access to computer data.[70] Article 18(1)(a) of the Cybercrime Convention requires each party to the Convention to

[66] Article 1(1) draft Regulation.

[67] Article 25 ff. CCC.

[68] Article 2(4) draft Regulation.

[69] Article 3(4) draft Regulation.

[70] See Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder access and jurisdiction: What are the options?, Report of the Transborder Group, adopted by the T-CY on 6 December 2012, T-CY (2012), p. 32. According to Belgian law, any provider of electronic communication services active in Belgium must, upon request of the public prosecutor, disclose identification data irrespective of whether or not the data is stored within Belgian territory. The Belgian Court of Cassation held that criminal sanctions for a failure to comply with such a request does not violate international law because the sanction and the request refer to a conduct within Belgian territory and, therefore, do not affect the territorial sovereignty of another state. (Art. 46 bis of the Belgian Code of Criminal Procedure; for the application to foreign providers see the judgment of the Hof van Cassatie [Belgian Court of Cassation], Judgment of 1 December 2015, P. 13.2082.N, Yahoo.). Similarly, the Irish Supreme Court found that an Irish court, if certain conditions were met, had the power to order the production of documents from an Irish company even if the required objects were located on foreign territory. (Supreme Court of Ireland, 25 January 2013, Walsh v. National Irish Bank, Appeal No. 267/2007, [2013] 1 ESC 2, para. 9.3.). Similarly the German legislator has adopted the Network Enforcement Act ("Netzwerkdurchsetzungsgesetz") that establishes a mandatory cooperation regime for service

adopt national laws under which relevant authorities can compel providers in their territory to disclose electronic data in their possession or control. This requirement contains no exception for data that a company controls but chooses to store abroad. A similar approach has been taken by the US in the CLOUD Act.[71] From a data protection perspective, EU data protection law applies regardless of where the data of persons concerned are stored. The applicability of the GDPR depends either on the fact that the data controller or processor is established within the EU, or on whether EU data subjects' data are processed, even when the controller or processor are not established on the territory of the EU (in which case they have to designate a legal representative in the EU).[72] The extended territorial scope of GDPR and the disappearance of location criteria aim at providing a more complete protection to EU data subjects regardless of where the company processing their data is established.

Considering that data is moved between servers in varying locations or—as in cloud computing systems—even scattered over several jurisdictions, reference to the place where the data is actually stored i.e. location of evidence, has become an outdated concept and irrelevant factor in determining enforcement jurisdiction. As some commentators put it, electronic data itself has become an "unterritorial" medium for which the concept of territoriality no longer fits.[73] This is a new development in criminal law. Jonson and Post 'predicted' over two and a half decades ago that "separated from doctrine tied to territorial jurisdictions, new rules will emerge to govern a wide range of new phenomena that have no clear parallel in the non-virtual world".[74] Yet it can be argued that, in the context of criminal justice and LEA's access to e-evidence, the concept of territorial jurisdiction itself has not become irrelevant; it simply is not—and need not—be linked to the location of the requested data. The 'de-territorialisation' or 'globalisation' of electronic-data and criminal evidence does not abolish the concept of territorial jurisdiction as such; it does not allow unlimited and uncontrolled cross-border access to electronic data in cyberspace. Instead, it encourages the development of the concept through replacing (or supplementing) the

providers whose services can be accessed from German territory. Network Enforcement Act of 1 September 2017, Bundesgesetzblatt 2017, part I, p. 3352.

[71] The first part of the CLOUD Act mooted the Supreme Court case of United States v. Microsoft Corp., 584 U.S. ___ (2018). Microsoft argued that the U.S. warrant had no legal force because the emails being sought were stored outside the United States, in Ireland. The United States argued that Microsoft could access the data from within the United States and thus the place where the data happened to be stored did not matter. The CLOUD Act resolved the legal issue, providing that the kind of compelled disclosure orders at issue in the Microsoft Ireland case apply "regardless of whether such communication, record, or other information is located within or outside of the United States".

[72] See Art. 3, in particular (2) and Art. 27 GDPR.

[73] See J. Daskal (2015) "The Un-Territoriality of Data", in Yale Law Journal, Vol. 125, p. 326; Bermann (2018) "Legal Jurisdiction and the Deterritorialization of Data", Vanderbilt Law Review, Vol. 71, p. 11.

[74] D. Johnson and D. Post (1996) "Law And Borders—The Rise of Law in Cyberspace" Stanford Law Review Vol. 48, p. 1367.

location of data by other grounds—connecting factors—that can be used to establish enforcement jurisdiction.[75]

E-evidence framework is a clear example of the development of the territorial jurisdiction concept and the evolvement of connecting factors. The E-evidence framework defines jurisdiction as follows: A SP offers services in the Union if it enables natural or legal persons to use its service in one or more MS(s) and has a substantial link to this MS respectively these MS(s).[76] This definition corresponds to the interpretation of Art. 18(1)(b) CCC.[77] Accordingly, a substantial link shall be considered to exist where the SP is established in the Union,[78] has a significant number or users in one or more MSs or targets its activities toward one or more MSs (by local advertising or advertising in a local language, by making an application ("app") available in the relevant national app store, providing customer service in a local language).[79] On the other hand, the provision of services in view of mere compliance with the prohibition to discriminate based on customers' nationality cannot be considered as targeting activities towards one or more MS(s).[80] The scope of the Commission's proposal is limited to data pertaining to services offered in the EU and does not allow for access to provider data related to services offered exclusively outside the EU.[81] In addition, the fact that EPOC and EPOC-PR can only be addressed in the context of criminal investigations implies a territorial link with the EU—either because the crime was committed in the territory of a MS or because the victim or the criminal is a citizen of a MS.

Currently, MSs follow divergent approaches on establishing enforcement jurisdiction for obtaining access to provider data. Connecting factors to establish jurisdiction are based on the location of data, the establishment of service providers, the place where the provider was offering services, the nationality of the person the electronic data pertain to etc. This fragmentation creates legal uncertainty for both the providers and the individuals concerned. According to the Charter of Fundamental Rights (Art. 8 CFR), legal certainty and transparency are essential to ensure that individuals are able to exercise their rights to data protection, to decide on whether to make use of a particular information or communication service and to take the risk of their personal data being accessed by law enforcement authorities. Overall the

[75] EU Parliament, Policy Department for Citizens' Rights and Constitutional Affairs (2018) Report p. 33. As in the proposed E-evidence framework, a territorial link can be based on other connecting factors such as the place where the service provider is established or where its services are offered.

[76] Article 2(4) draft Regulation, Art. 2(3) draft Directive.

[77] According to the Cybercrime Committee's guidance note.

[78] Article 2(4) draft Directive.

[79] Recital (13) draft directive.

[80] Recital (13) draft directive, referring to Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market, O.J. L 60 I/1.

[81] Article 3(3) draft Regulation.