The Digital Unfitness of Mutual Legal Assistance

Busser, E. de

BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS 28 (2017) 161-179

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

The Digital Unfitness of Mutual Legal Assistance

Els De Busser
Assistant Professor Cyber Security Governance, Institute of Security and Global Affairs, Leiden University
e.de.busser@fgga.leidenuniv.nl

Abstract

Any crime could generate digital evidence. That is a reality law enforcement authorities across the world need to face. The volatile and "unterritorial" nature of the evidence means that international cooperation in criminal matters is confronted with new questions. One of these questions is whether the traditional cooperation mechanism, mutual legal assistance, is a viable way of working. Due to its time-consuming and cumbersome functioning combined with the lack of a faster alternative, countries have developed unilateral and extraterritorial methods of evidence gathering. This paper zooms in on this development and the risks it entails.

Keywords

digital evidence – international cooperation – criminal law – mutual legal assistance – mutual recognition

Sketching the Problem

In 1990 Christine van den Wyngaert stated that "it is fashionable nowadays to discuss the problems that arise from the application of general human rights to extradition".[1] Ten years later, Robert J. Currie expanded this statement to

1 C. Van den Wyngaert, 'Applying the European Convention on Human Rights to Extradition: Opening Pandora's Box?', in The International and Comparative Law Quarterly, 1990, no. 4, p. 758.

include other forms of international criminal cooperation as well.[2] The reasoning behind both statements was fuelled by questions brought before the European Court of Human Rights (ECtHR) on the discretion of a central authority – in most states the Ministry of Justice – to refuse the extradition of an individual to the requesting state for the purpose of criminal prosecution or sentencing. Extradition, just like any other type of assistance in criminal matters, can be refused under specific circumstances. Surprisingly however, human rights compliance by the requesting state is not one of the grounds for refusal traditionally included in bilateral and multilateral agreements covering extradition and mutual legal assistance. This is surprising considering the responsibility a state's central authority could incur when transferring an individual to a state that has a poor human rights track record. In a number of landmark cases the ECtHR has ruled on the modalities of such decisions by the requested state. Questions on possible human rights based grounds for refusal of information exchange have not found their way to the ECtHR that easily. Obviously, the stakes are much higher when the transfer of a person is concerned as opposed to the transfer of witness statements, criminal record copies or the report on a house search conducted in the requested state. Yet, not paying sufficient consideration to the human rights exception in a mutual legal assistance context would downgrade the importance of human rights such as the right to a private life and the right to a fair trial.

In this article I build upon the perspectives developed by both aforementioned scholars and expand their reasoning to the current reality of cross-border digital evidence. Evidence of crime is located where the crime took place and where the criminal was. That sounds easy enough in an analogue setting. The crime scenes that are often depicted in numerous movies and series paint a romanticized picture of teams of inspectors tracing and analyzing microscopic fibers, partial fingerprints, DNA samples and fragments of material to solve cases – even cross-border cases – in a record amount of time. The reality is far less glamorous and far more time-consuming. Criminal investigations with links to more than one state are likely to trigger some form of cross-border cooperation, known as mutual legal assistance (MLA) in criminal matters. In most cases this means a request for a witness hearing or house search to be conducted abroad, a request for a copy of a criminal record or a bank statement. The modalities of such cooperation and the conditions under which it can take place are laid down in a number of multilateral and bilateral

2 R.J. Currie, 'Human Rights and International Mutual Legal Assistance: Resolving the Tension', in Criminal Law Forum, 2000, no. 11, p. 143.

agreements allowing states to perform several checks on the incoming request from another state before deciding whether to follow up with the request. Grounded in diplomatic relations and the protection of state sovereignty, MLA gives the requested state the chance to refuse to cooperate in prosecuting behavior it may not consider to be a criminal behavior, or behavior it has already prosecuted and sentenced by final judgment (*ne bis in idem* principle). Thus, even when MLA originated as protecting states' interests, it has grown to include a significant human rights protective function.

Still, it seems as if the traditional mechanism of MLA is losing ground quickly because of its slow and cumbersome way of working. With surveys showing that it takes authorities an average of ten months to react to a request for MLA[3] – in some cases, no reaction is received at all by the requesting authority – individual states, as well as the EU institutions, have sought faster alternatives. Ten months is slow in any criminal investigation – even in a domestic setting – but it is unworkably slow when the evidence is digital rather than tangible.

Indeed, the rapid increase of digital evidence for all types of criminal offences – not just computer-related offences – emphasizes the slowness and general inadequacy of the traditional cooperation system. Digital evidence introduces not only a volatile type of information that can be highly relevant to criminal investigations, but also presents a world of territorially organized national criminal laws with the inherently unterritorial[4] world of digital data. Combining the two seems to push states towards a move away from MLA. Recent efforts have been directed at solving the problem of slow cooperation, but seem to jump over the question of human rights protection. This article will analyze whether the latest initiatives by the European Commission and by the United States are effectively eating away at the protective function of MLA in favor of faster cooperation. Offering the necessary context, the first section will narrow in on the roots of MLA and the interests that it protects: the state's interests, the individual's interests or both. Secondly, the paper will examine the EU mutual recognition legal instruments that have largely replaced MLA between EU member states, and will also look across the Atlantic and study the US CLOUD Act in the same sense. The concluding remarks will highlight the arguments surrounding the debate about whether or not MLA can be united with digital evidence.

3 New EU Rules to Obtain Electronic Evidence, European Commission (Apr. 17, 2018), http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

4 J. Daskal, *The Un-Territoriality of Data*, in Yale Law Journal, 2015, no. 125, pp. 326–98.

Whose Rights are Protected?

Before examining how the European Commission and the US government are moving away from traditional MLA in criminal matters, it is necessary to first clarify the origins of the system. The common thread in sketching the background of mutual legal assistance for the purpose of this article is the question of whose interests are protected? Is it the purpose of MLA to protect the interests of the state or the interests of the individual(s) involved in a cross-border criminal investigation or both?

Origins of MLA

Few cooperative mechanisms have such a long, yet under recognized history as MLA. In fact, when one speaks of the so-called wider MLA, that includes extradition,[5] more sources seem to surface on where this particular kind of cooperation comes from. It shows the tight connection between extradition and other forms of interstate cooperation in criminal matters. Extradition between sovereign rulers has a long history. The oldest known extradition provisions in a treaty were agreed between Egyptian Pharaoh Ramses II and Hittite King Hattusili.[6] Even in these ancient provisions, reciprocity between the two agreeing parties was explicitly mentioned. This is not a coincidence. When one sovereign transfers a fugitive back to his or her home country, the other returns the favor. It is still today a principle that lies at the foundation of both extradition and MLA. It shows that the original purpose of such provisions was to protect the interests of the state and not of the individual(s) involved. A second feature in the history of MLA that demonstrates that the protected interests are those of the state is the importance of diplomatic traffic as a vehicle for MLA requests. Even today, the possibility to transfer MLA requests from one country to the other via the diplomatic channel remains in the older but still used agreements on MLA.

MLA and extradition were developed alongside each other, although during the preparatory stages of the first multilateral agreement on MLA, under

5 As opposed to so-called small MLA or MLA in the narrow sense which includes all cooperation in criminal matters that are not extradition, transfer of proceedings and transfer of sentenced persons. For the purpose of this article MLA will be used in the narrow sense.

6 See H. Nilsson, 'From Classical Judicial Cooperation to Mutual Recognition', in Revue International de Droit Pénal, 2006, no. 1, pp. 53–54 and S. Langdon and A.H. Gardiner, 'The Treaty of Alliance between Ḫattušili, King of the Hittites, and the Pharaoh Ramesses II of Egypt', in The Journal of Egyptian Archaeology, 1920, Vol. 6, No. 3, pp. 192–193.

the auspices of the Council of Europe (CoE) in 1959, a clear split was made between extradition and MLA. The authors of the 1959 CoE MLA Convention felt that MLA should be independent of the former in that extradition should be granted even in cases where extradition was refused.[7] Attention had now turned more towards the individual and his or her rights during a cross-border criminal investigation. The trend towards increased protection of human rights seems to have originated in the immediate post-World War II era when in general more consideration was given to human rights.[8] Nevertheless, this still happened in a rather humble manner and that becomes clear when looking at the provisions stating on which grounds a requested state can refuse to cooperate. For the purposes of this article only those grounds for refusal that are considered traditionally related to extradition but often make an appearance in the MLA context are examined: the political offence exception, the sovereignty and public order clause, the *ne bis in idem* principle and the double criminality condition.[9]

Who is Protected by a Refusal to Cooperate?

The 1959 CoE MLA Convention provided only two grounds for refusal. The first was assistance for political and fiscal offences, although by protocol of 1978 the ground for refusal of assistance for fiscal offences was removed. In EU legal instruments, the use of the political offence exception has declined in general. Instead, prominence has been given to mutual trust, for example through the European Arrest Warrant, as a basis for almost automatic[10] recognition by member states' authorities of each others' judicial decisions. With regard to political offences, protection against prosecution for such offences in the home state could obviously be viewed as human rights protection but at the same time it serves the interests of the state in the context of international relations. By blocking cooperation on a perceived political offence, the requested (or executing) state is not only refraining from helping the requesting (or issuing) state's government to pursue its political goals, it is also sending a clear message to the requesting state that the prosecution of the individual in question crosses an important line.

7 Council of Europe, ETS 30, Convention Mutual Assistance in Criminal Matters, Explanatory Report p. 2.

8 M.C. Bassiouni, International Extradition Law, Oxford University Press, 2014, p. 6.

9 See also R.J. Currie, 'Human Rights and International Mutual Legal Assistance: Resolving the Tension', in Criminal Law Forum, 2000, no. 11, p. 160.

10 The phrase "almost automatic" refers to a limited amount of grounds for refusing an incoming European Arrest Warrant by the executing state.

The second ground for refusal can be seen in contemporary MLA agreements and is formulated in a wider manner:[11] "assistance may be refused if the requested party considers that execution of the request is likely to prejudice the sovereignty, security, *ordre public* or other essential interests of its country".[12] Obviously it is the more sensitive type of cases that will trigger such refusals and the requesting state can in most cases anticipate the requested state's reaction. Prior consultation can therefore be of significant help.[13] Born out of concern for having to transfer evidence related to national security or economic interests of the state, the clause "essential interests" is considered wide enough to also cover human rights matters.[14] Relying on this ground for refusal could thus have the effect of protecting the individual. Yet, its *raison d'être* is the interests of the state. Both the prominent role of sovereignty, as well as the far-reaching scope of the ground for refusal are evident. It is important to note that applying this ground of refusal is at the discretion of the requested state, as it is not formulated in a mandatory sense.

Refusing cooperation for reasons of a final judgment ruled on the same criminal conduct in another state – the *ne bis in idem* principle – is a ground for refusal that is much less frequently used in the context of MLA than in comparison to extradition. The 1959 CoE MLA Convention and its protocols do not even contain a ground for refusal of cooperation based on *ne bis in idem*.[15] The same approach was taken in the 2000 EU MLA Convention and its protocol. It is only an optional ground for non-execution of a European Investigation Order that is currently the legal instrument used by EU member states for most requests for evidence.[16] More on mutual recognition orders for evidence will follow later in this article. The applicable multilateral legal instruments covering the transfer of a person for the purpose of prosecution or the execution of a sentence – the CoE 1957 Extradition Convention and the EU's Framework

11 It is for example included in Article 4 of the UN Model Treaty on Mutual Assistance in Criminal Matters, UN General Assembly, A/RES/45/117, 68th plenary meeting, 14.12.1990.

12 Article 2 Council of Europe, ETS 30, Convention Mutual Assistance in Criminal Matters.

13 K. Prost, Practical solutions to legal obstacles in mutual legal assistance, in Denying safe haven to the corrupt and the proceeds of corruption, ADB/OECD, 2006, pp. 33–34.

14 R.J. Currie, 'Human Rights and International Mutual Legal Assistance: Resolving the Tension', in Criminal Law Forum, 2000, no. 11, p. 161.

15 However several states (e.g. Armenia, Denmark, Iceland and Norway) have made a declaration stating that they reserve themselves the right to refuse cooperation if the individual subject to the request has been convicted for the same fact by a final judgment on a domestic level.

16 Article 11, 1, d) of the Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, O.J. L 130, 01.05.2014.

Decision on the European Arrest Warrant – do include *ne bis in idem* as a mandatory ground for refusal as long as final judgment has been passed. A significant conclusion drawn from this by John Vervaele[17] is that there is no right to *ne bis in idem* for the individual. On the contrary, it is a barrier for cooperation between states and thus protects the interests of the state. This may make sense considering that the origins of the principle lie in sovereignty and the legitimacy of the state and its legal system, as well as in the respect for the *res judicata* of final judgment, rather than in the protection of human rights. However, Article 54 of the Schengen Implementation Agreement and Article 50 of the EU Charter create a subjective right to *ne bis in idem* for EU citizens.[18] Even when it is a derogable right, it has the substantial effect of protecting the rights of the individual involved.

Similar to the *ne bis in idem* principle, the ground for refusal based on dual or double criminality is more common in the field of extradition than it is in MLA. Refraining from cooperating with another state because its request is based on conduct the requested state does not consider a criminal offence, has a diverse application in the European and EU legal instruments. State parties to the CoE MLA Convention, for instance, may reserve the right to refuse carrying out an MLA request when the offence in question is not a punishable offence in both the requesting and requested state, but only for search or seizure of property. In the most recent EU legal instruments governed by the principle of mutual recognition such as the European Investigation Order, a list of 32 offences was developed that are considered to be so "mutual" among the member states that no dual criminality check should even be made. A few exceptions apply however. Here, the main question is whose interests are protected by the ground for refusal based on dual criminality. Starting from the idea that a state's criminal policy as well as its ideological, historical, cultural or religious identity is demonstrated by what the state considers to be a crime, one could view it as a state's assertion of its sovereign legislative power to refuse to cooperate in the investigation of conduct it does not consider criminal. The above-mentioned list of 32 offences in the EU's mutual recognition instruments assumes advanced levels of harmonization among the member states' national substantive criminal laws, making it unnecessary to assess dual criminality. In extradition cases it is far more clear that the double criminality condition protects the rights of the individual who found refuge in a state that is not transferring him or her to the requesting state for conduct it does not

17 J.A.E. Vervaele, 'Ne Bis In Idem: Towards a Transnational Constitutional Principle in the EU?', in Utrecht Law Review, 2013, Vol. 9, no. 4, p. 213.

18 Ibid., pp. 212–229.

consider an offence. The person will be safe from prosecution as long as he or she can remain in the requested state. When obtaining cross-border evidence is concerned, however, it is possible that the individual will be prosecuted regardless of the delivery of the evidence. Only in the off chance that the reason for the MLA request is evidence that is essential for a successful prosecution, the criminal proceedings in the requesting state may be hindered. Therefore, the dual criminality condition seems to protects the interests of the state rather than the interests of the individual.

The above-examined grounds for refusal have not been drawn up out of concern for the safeguarding of individuals' human rights. Even the political offence exception – where the individual is the main focus – has been a point of fundamental discussion in international cooperation. Before examining whether the protective mechanisms of MLA are at risk when digital evidence is concerned, let us first take a critical look at the alternatives developed for cross-border transfer of evidence by the EU institutions and the US.

Alternative Cooperation Mechanisms

Both the European Commission and US Congress have been active the previous years in searching for faster, more productive ways of obtaining cross-border evidence. Frustrated by the unpredictable consequences of sending out an MLA request, governments on both sides of the Atlantic looked for a less time-consuming, more straightforward way of dealing with crime that is increasingly more international. The introduction of digital material as potential evidence in a criminal investigation accelerated the search for alternative methods.

EU Initiatives to Replace MLA

The establishment of the EU as an economic union introduced the conferral of legislative powers by the member states to the supranational institutions of the EU in commercial matters. For criminal matters, member states were much more reluctant to see legislative power in the hands of the EU institutions. This hesitancy, caused by the above-mentioned relationship between a country's criminal law and its identity and sovereignty, could however not be maintained in light of the rise of cross-border crime which necessarily demands increased cooperation. Conferring only part of their legislative powers in criminal law, member states still held control over rules on evidence such as the admissibility of evidence and the weighing of evidence but agreed to a new form of faster cooperation based on the assumption of mutual trust. The

EU legislative bodies have adopted a number of legal instruments by now. Mutual recognition instruments are not without problems and the compliance of particular member states with human rights has been questioned more than once. In addition, member states have been relying on alternative methods to obtain cross-border digital evidence, sometimes unilaterally. A new set of e-evidence proposals[19] aims to iron out the current differences between member states' systems.

Mutual Recognition

In times when Brexit preparations are in full swing it may seem ironic, but it was the UK's presidency of the European Council in 1998 that initiated the first talks on using the principle of mutual recognition to improve judicial cooperation in the context of cross-border crime.[20] Aiming to improve MLA's functioning, which suffers from a lack of enforcement, speediness and in some cases political will in ratifying conventions or in executing individual requests, the European Council in Tampere called mutual recognition the cornerstone of judicial cooperation in civil and criminal matters.[21] The idea sounds simple: if all members of the Union have mutual trust in each other and in each other's criminal justice systems, they should have no difficulties recognizing each other's judicial decisions as their own. A state that receives a foreign judicial decision for execution in its domestic system then no longer needs to assess the legality, necessity and proportionality of the decision and the measure that should be carried out, because this has already been done by the issuing state.[22] The traditional conversion mechanism of a foreign decision into a domestic one is thus avoided. The principle of mutual recognition introduces an almost blind recognition of foreign decisions. Almost, because a limited number of grounds for refusal still remain.

Faith in this new concept of cooperation seemed high at first and stimulated by the momentum of the post-9/11 era, the European Arrest Warrant (EAW) was adopted as the first mutual recognition instrument.[23] Replacing

19 See footnotes 37 and 38.

20 European Council, Presidency Conclusions, 15–16 June 1998, §39. See also H. Nilsson, footnote 6, p. 56.

21 European Council, Presidency Conclusions, 15–16 October 1999, §33.

22 L. Bachmaier-Winter, 'European investigation order for obtaining evidence in the criminal proceedings', in Zeitschrift für Internationale Strafrechtsdogmatik, 2010, no. 9, pp. 581–582.

23 Framework Decision on the European Arrest Warrant and the Surrender Procedures between Member States, O.J. L 190, 18.07.2002.

extradition between EU member states with a standardized form ordering – not requesting – the surrender of a person, the EAW did not even contain a dual criminality check for a list of 32 offences. Dual criminality is assumed for these crimes for as far as they are punishable with a maximum custodial sentence of minimum three years. Mandatory grounds for refusal in the EAW are restricted to cases of amnesty, young age and *ne bis in idem*. The list of grounds for optional non-execution of the EAW is longer but the main absentee is a ground for refusal based on human rights. Whereas extradition procedures became increasingly protective of the rights of the individual concerned,[24] the assumed trust between EU member states that forms the foundation of mutual recognition swept away the need for a human rights based ground for refusal.

The drawback of such assumption became painfully clear in the joined Aranyosi-Caldararu cases before the Court of Justice. A German prosecutor questioned the detention conditions in Romania and Hungary in the context of an EAW for the surrender of two individuals arrested in Germany.[25] The Court ruled in favor of a refusal of the EAW execution in cases of a real risk of inhuman or degrading treatment in the issuing state. The assumed mutual trust seemed to be crumbling under the pressure of certain member states that do not have a clean human rights track record. Furthermore, the ground for refusal based on dual criminality showed its weakness when Catalan leader Carles Puigdemont was the subject of an EAW issued by the Spanish authorities to the German authorities.[26] Accused of several criminal offences, including embezzlement and rebellion, it was the latter offence that was unknown in the German criminal code. The competent German court ruled to not allow surrender for rebellion but to allow it for embezzlement of public funds.[27]

Recognizing the need for a better balance between effective cooperation in criminal matters and human rights, a small group of member states tried to do better when drafting the European Investigation Order (EIO). Still applying the mutual recognition principle, the EIO aims to replace most[28] of the MLA convention by offering a fast working order for evidence in another member state

24 See footnote 8.

25 CJEU, Joined Cases C-404/15 and C-659/15 PPU, 05.04.2016.

26 L. Bachmaier-Winter, 'Fundamental Rights and Effectiveness in the European AFSJ', in eucrim 2018, no. 1, p. 61.

27 Press release by the Oberlandesgericht for the State of Schleswig-Holstein, 12.07.2018.

28 Those MLA provisions relating to measures not falling in the scope of the EIO will remain applicable. Also, Ireland and Denmark are not taking part in the EIO so for cooperation involving these countries the unpopular European Evidence Warrant remains valid.

with short deadlines and a wide scope.[29] Investigative measures such as house searches, witness hearings, monitoring bank accounts and criminal records or other types of information from the executing authority, can all be ordered by using an EIO. Unlike the EAW, the EIO text does include an (optional) ground for non-execution when there are substantial grounds to believe that the execution of the investigative measure would be incompatible with the executing state's obligations in accordance with Article 6 of the Treaty on European Union (TEU), which refers to the ECHR and the Charter. This is a clear ground for refusal based on human rights. It would for instance block the obtaining of evidence without due compliance with the right to privacy and the exceptions allowed in the context of a criminal investigation.

Circumventing the Executing Authority

In the 2015 European Agenda on Security,[30] the European Commission recognized issues surrounding access to digital evidence but still placed these issues under the title of cybercrime. This shows a rather limited view of digital evidence since any type of crime can – and will – generate digital evidence, not just the crimes that are labeled as cybercrime. Nevertheless, the Commission's point on the need for a mechanism to deal with digital evidence was more than valid. Even in simple domestic criminal investigations, the use of cloud computing by natural and legal persons could require cross-border seizing of evidence, potentially even outside the EU. Additionally, digital evidence is highly volatile. It can be moved across jurisdictions, changed and destroyed in a matter of seconds.[31]

Since the above-mentioned EIO is faster than MLA,[32] but a cooperation mechanism between judicial authorities that is still too slow for comfort, EU member states started developing their own solutions for obtaining digital evidence. In September 2016 a questionnaire held by the Commission services revealed the lack of a common approach to obtain cross-border access to digital evidence by the member states.[33] They either went directly to the Internet

29 With the exception of joint investigation teams and police surveillance, the EIO allows for most forms of evidence gathering. Directive regarding the European Investigation Order in criminal matters, O.J. L 130, 01.05.2014.

30 COM(2015) 185 final.

31 CETS no. 185, Cybercrime Convention, Explanatory report, §256.

32 See: New EU Rules to Obtain Electronic Evidence, European Commission (Apr. 17, 2018), http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

33 See the results of a questionnaire by the Commission services in September 2016 revealing the lack of a common approach to obtain cross-border access to digital evidence: Technical Document: Measures to improve cross-border access to electronic evidence for

service provider with a request to cooperate or by means of direct cross-border access to the digital evidence. These unilateral moves could be explained by a clear need for access to digital evidence stored in other (member) states, combined with the lack of a proactive approach by the European Commission. Unilateral here refers to not requiring the assistance of the state where the evidence is stored.

By jumping over the state where the digital evidence is stored, the requesting state is circumventing potential grounds for refusal. In the case of direct requests to an Internet service provider the member states answering to the aforementioned questionnaire, did not agree on whether such direct requests should be mandatory – seven member states think they are – or voluntary. Even when the request was deemed mandatory, enforcement is doubtful.[34] An Internet service provider is a company and not an authority, so invoking grounds for refusal as we know them from MLA and mutual recognition would not be a task for them. It is also not in the interests of a company to refuse cooperation based on, for instance, double criminality or *ne bis in idem*. Moreover, no company would have the means or the know-how to thoroughly assess such grounds.

It would however be in the interests of any company to avoid a conflict of laws. Companies receiving requests for digital evidence issued by the authority of another state could be prohibited by their own jurisdiction to not hand over such information. In the case that they comply with the laws of their own state, they would trigger liability for refusing to execute a legal order if the state in question considers the request mandatory.[35] Yet legal frameworks for enforcing such orders are often lacking.[36] It is this legal impasse that the European Commission attempted to remedy by presenting two proposals in April 2018.

E-evidence Proposals

The proposals presented by the European Commission consist of a proposed regulation on European Production and Preservation Orders for electronic

criminal investigations following the conclusions of the Council of the European Union on improving criminal justice in cyberspace and Questionnaire on improving criminal justice in cyberspace – Summary of responses: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

34 Ibid.

35 Belgium, Cyprus, Spain, Portugal, UK, France and Lithuania responded to the questionnaire by stating they consider direct requests to Internet service providers mandatory.

36 Only Sweden, Cyprus and Malta have such regulation in place.

evidence in criminal matters[37] and a proposed directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[38] This brief analysis will focus on the proposed regulation, since by introducing a production order for data the Commission offers authorities the option of directly obtaining data from a EU-based company or from a company's legal representative within the EU. Because the proposed preservation order implies merely the safeguarding of the data in view of a subsequent order for transferring the data – similar to a freezing order followed by a confiscation order – I will here narrow my focus to the production order only.

The proposed mechanism would offer legal certainty to the companies that find themselves in the above-described legal impasse because such companies can – in accordance with Article 15 of the proposed regulation – object to an order for data in case of a conflict of laws. Following such objection, the requesting authority should revise the request or ultimately bring the matter to a judge. Besides a conflict of laws, in accordance with Article 14 of the proposed regulation, the company in question could also refuse to hand over requested data based on a human rights violation. If the order for data manifestly violates the EU Charter of Fundamental Rights and Freedoms or is manifestly abusive, the company should send the order to the competent enforcement authority in the member state where the company is based. This means that companies become the first line responders for conflicts of laws and for human rights breaches, rather than a Ministry of Justice, as is the case in traditional MLA, or a judicial authority, as is the case in other mutual recognition legal instruments.

On 12 December 2018 the Council reached a general approach on the proposed regulation containing significant changes to the Commission's proposal.[39] The above-discussed mechanism of allowing companies to decide on the grounds for refusal is removed from the text of the proposed regulation. It is

37 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM (2018) 225 final, 17.04.2018. See also the elaborate opinion of the Meijers Committee: Standing Committee of experts on international immigration, refugee and criminal law, CM1809 Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 18.07.2018.

38 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, (2018) 226 final, 17.04.2018.

39 Council of the EU, 15292/18, Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters – general approach, 12.12.2018.

however not replaced by an alternative. Such removal makes the situation even worse since now no one except the issuing authority is made responsible for assessing the production orders on their conformity with human rights. If for example an issuing authority submits a production order to a company for data from a dynamic IP address that can potentially affect hundreds of people, the recipient company has in accordance with the Council's general approach no possibility to object based on a lack of proportionality. For that reason it is highly unlikely that the proposed regulation will be adopted as it stands now. Yet, the reintroduction of Article 15 is not a good option. I explain here why companies should not be first line responders for conflicts of laws and human rights breaches.

Three consequences of giving companies such responsibility in the context of interstate cooperation in criminal matters are particularly concerning.[40] First, the proposed regulation effectively gives companies the role of a public authority. Where even direct contact between police authorities of two states was unthinkable in MLA until the 1990 Schengen Implementation Convention, we now see direct cross-border transfers of evidence from companies to law enforcement authorities being institutionalized. The reason why a central authority – mostly the Ministry of Justice of a country – is the intermediary for incoming requests for MLA in the 1959 CoE Convention is the protection of sovereignty and indirectly the protection of their international relations. Answering the question of whether or not to deliver assistance to a foreign criminal investigation also means judging the quality of the requesting state's criminal justice system, especially when human rights compliance is concerned. This is not the kind of responsibility that should be placed in the hands of a company. Besides the fact that companies have economic interests, the companies in question are quite often US based companies, even when acting through a legal representative in the EU. As the first line responder to a production order for data, if the legal representative does not alert the competent enforcement authority of the member state where he or she is based, no other public authority but the issuing authority will ever get to see the production order. Effectively, this means that an EU based company or an EU based legal representative of a third state's company has the responsibility to decide whether or not the order by a member state is in line with human rights or not. Keeping in mind the human rights questions triggered by recent European Arrest Warrant

40 See also Meijers Committee: Standing Committee of experts on international immigration, refugee and criminal law, CM1809 Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 18.07.2018.

cases, and keeping in mind the activation of the Article 7 TEU procedure against two member states, such a decision carries too much weight to be put in the hands of a company.

Second, companies are not equipped to be placed in such position. In addition to the argument made concerning their economic interests, companies – especially Small and Medium Sized Enterprises (SMEs) – would have to spend a considerable amount of their resources to scrutinize potential grounds for refusal for every incoming request for data. Also related to the first concern, and not to be underestimated, is the risk that companies may not be able to make a proper assessment of the grounds for refusal.

Third, an imaginable liability issue could arise for any company that does not object or refuse a request for data where it should have. A consumer whose data was transferred by a service provider in reaction to an order for digital evidence that was manifestly breaching the right to data protection[41] could first of all submit a legal claim against that company. Furthermore, the evidence resulting from it would be inadmissible in the subsequent criminal proceedings and potentially – depending on the evidence laws of the member state and whether or not the fruit of the poisonous tree doctrine[42] is supported – endanger all further evidence derived from it. Such action could therefore result in possible legal claims from victims as well.

A considerable added value of the proposed regulation obviously lies in the recognition and organization of a faster mechanism for obtaining data. Orders for preserving digital evidence should be carried out without undue delay in order to prevent manipulation, destruction or moving of the data, whereas production orders should in principle be carried out within ten days upon receipt of the order. In urgent cases this can even be shortened to six hours. This is a far cry from the average of ten months for the execution of an MLA request and the average of 120 days for receiving the results of an EIO.[43] The proposed regulation thus has significant potential in offering a solution to a challenging problem: the obtaining of cross-border digital evidence. However, by giving companies the responsibility to check the grounds for refusal of an order for data without necessarily passing by a Ministry of Justice or a judicial authority

41 Article 8 EU Charter of Fundamental Rights and Freedoms.

42 The fruit of the poisonous tree doctrine refers to the excluding of evidence that was obtained illegally. Not just the illegally gathered evidence is excluded but also all evidence derived from it.

43 New EU Rules to Obtain Electronic Evidence, European Commission (Apr. 17, 2018), http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

first, one of the building blocks of interstate cooperation in criminal matters is effectively erased.

Let's imagine that the case surrounding Carles Puigdemont, and the EAW issued by the Spanish authorities to the German authorities, evolved around digital evidence. Imagine that instead of an EAW, a production order was issued for content data on Puigdemont's communication to a service provider based in Germany. The company in question would have had to assess that rebellion was indeed a criminal offence punishable in Spain by a custodial sentence of a maximum of at least three years. That would be a fairly uncomplicated check. As there is no dual criminality requirement in the proposed regulation,[44] the company would not have to check whether rebellion is a criminal offence in accordance with German law. It is also unlikely that the production order would be refused based on a manifest violation of human rights or a conflict of laws. Hypothetically, a German service provider could thus, in accordance with the proposed regulation, assist the Spanish authorities to prosecute Carles Puigdemont for an offence the German court refused to surrender him for.[45]

US Initiatives to Replace MLA

On any given day, consumers worldwide use the communication services offered by a rather small number of US based companies. This makes it useful to take a look at the legal framework relating to digital evidence in the US, where new legislation was also adopted in 2018. The so-called Microsoft Ireland case was the trigger for a new act that looks fairly similar to the proposed EU regulation on e-evidence.

Microsoft Ireland Case

Companies storing massive amounts of data on users' communications often have data centers in different parts of the world. Microsoft has a data center based in Ireland, where it stores most of its European email traffic. When the US headquarters of Microsoft received a warrant from the US authorities to transfer data concerning a specific email account, Microsoft was not willing to

44 See also V. Franssen, 'The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?', in European Law Blog: http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

45 Press release by the Oberlandesgericht for the State of Schleswig-Holstein, 12.07.2018: https://www.schleswig-holstein.de/DE/Justiz/OLG/Presse/PI/201803Puigdemontenglisch.html.

hand over that part of the requested data that was stored in Ireland.[46] Interestingly, both the company and the US authorities agreed that US national law does not apply outside American territory. The core of the arguments though was the question whether the control of a company over the data determines their location. Because Microsoft could technically access the data from the US, the US authorities claimed the warrant was sufficient. The opposite – and Microsoft's view – would necessitate an MLA request to the Irish authorities. Most likely the 2001 bilateral MLA Treaty between the US and Ireland would then be applicable, complementary to the 2003 EU-US MLA Agreement. Relying on a MLA request in this case would have put the assessment of any grounds for refusal in the hands of the receiving Irish authority.

CLOUD Act

The Microsoft Ireland case is an example of the above-mentioned conflict of laws. In particular the US Electronic Communications Privacy Act ("ECPA") blocks the disclosure of content data in many circumstances of cross-border transfer. In light of a draft data sharing agreement between the US and the UK[47] US Congress adopted the so-called CLOUD (Clarifying Lawful Overseas Use of Data) Act.[48]

The significance of the CLOUD Act for EU law enforcement authorities is that it allows US based companies such as Microsoft or Apple to disclose data to them regardless of where these data are physically stored as long as the data do not relate to US citizens or residents. When for example a French authority needs data on the email traffic between a French and a Belgian citizen via a Microsoft email account, there is a chance that these data are stored on the server in Ireland but they may as well be stored on a server in Brazil. Pursuant to classic interstate cooperation, this would require an MLA request. Yet in accordance with the CLOUD Act, MLA requests are no longer needed if the requesting state is "labeled" by the attorney general as a state that has adequate substantive and procedural laws on cybercrime and electronic evidence in place, demonstrated respect for the rule of law and principles of non-discrimination and adherence to international human rights obligations – a mechanism that works similar to the adequate level of data protection presented by the EU in Directive EC/46/95, now replaced by the General Data Protection Regulation. Instead of grounds for refusal that could be invoked for

46 U.S. v. Microsoft, 584 U.S. 1 (2018) (per curium).

47 M. Murgia, 'UK–US pact will force big tech companies to hand over data', in Financial Times, 23.10.2017: https://www.ft.com/content/880bc2ae-b980-11e7-9bfb-4a9c83ffa852.

48 CLOUD Act, H.R. 4943, 115th Cong. (2018).

an individual data transfer and could protect the interests of the person and the state involved, the CLOUD Act builds in more attention for human rights protection by an ex ante check of a state's criminal justice system. After all, the assessment the attorney general should make is strongly concerned with the risks of data usage for the data subject. Once a state has passed this hurdle, the company controlling the data should make the transfer regardless of where the data are located. In the previous example, France would then receive the data from Microsoft even when the data would be stored on a server in Brazil and even though the Brazilian Ministry of Justice is unaware of the matter. Would the Brazilian Ministry of Justice take an interest? In most cases this is at least doubtful. However, in those cases where the use of the data would likely prejudice Brazil's sovereignty, national security, public order or the economic interests of the country, it is highly likely that the Ministry would want to invoke such ground for refusal. Simply because Microsoft is a US based company, a country's interests could be bypassed.

Digitally Unfit

The US CLOUD Act may not put a company in a strategic position in the same way that the proposed regulation of the European Commission does, but the effect of circumventing the safeguards built into the MLA cooperative mechanism is alarming.[49] The attorney general's ex ante assessment in the form of an American version of the EU adequacy requirement does not remove concerns related to the interests of the possible countries involved. The country where the data are located – both in the proposed EU regulation and the US CLOUD Act – has no voice in the matter of what is done with the data in the context of a criminal investigation.

Where the US CLOUD Act leaves the decision on "safe" requesting countries in the hands of the attorney general, the proposed EU regulation lets the company involved decide on the grounds for refusal of the request for digital evidence. The Council however removed this review mechanism by companies without offering an alternative, leaving the data production orders without assessment by anyone but the issuing authority. These are different approaches with the same effect: safeguards developed under the traditional MLA system are dismantled. The reasons are clear. MLA is too slow, too cumbersome,

49 See also K. Rodriguez, 'The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom, Electronic Frontier Foundation', 09.04.2018: https://www.eff.org/nl/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.

possibly too dependent on governments whereas digital evidence is volatile, unterritorial and in the hands of private companies. How to reconcile the two means to involve private actors in a mechanism that is essentially manned by public authorities? Yet this involvement should not lead to these private companies taking on the responsibilities of a Ministry of Justice or judicial authority. Keeping the grounds for refusal checks in the hands of such authorities is essential for safeguarding the interests of the states and individuals involved. With regard to the interests of the state where the data are located, an assessment of the effect on its sovereignty, national security or essential interests seems like a bare minimum requirement. Moreover, MLA can and should be made into a faster process while keeping these safeguards by shortening deadlines and making it a valid alternative for unilateral direct requests.