Articles

EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow

By Els De Busser[*]

Abstract

Criminal offenses with the most different modi operandi and levels of complexity can generate digital evidence, whether or not the actual crime is committed by using information and communication technology (ICT). The digital data that could be used as evidence in a later criminal prosecution is mostly in the hands of private companies who provide services on the Internet. These companies often store their customers' data on cloud servers that are not necessarily located in the same jurisdiction as the company. Law enforcement and prosecution authorities then need to take two steps that are not exclusive for evidence of a digital nature. First, they need to discover where the data is located—with which company and in which jurisdiction. Second, they need to obtain the data. In considering digital evidence, the last step, however, is complicated by new issues that form the focus of this paper. The first concern is the practice by companies to dynamically distribute data over globally spread data centers in the blink of an eye. This is a practical concern as well as a legal concern. The second issue is the slowness of the currently applicable international legal framework that has not yet been updated to a fast-paced society where increasingly more evidence is of a digital nature. The slowness of traditional mutual legal assistance may be no news. The lack of a suitable legal framework for competent authorities that need to obtain digital evidence in a cross-border manner, nonetheless, creates a landscape of diverse initiatives by individual states that try to remedy this situation. A third issue is the position that companies are put in by the new EU proposal to build a legal framework governing production orders for digital evidence. With companies in the driver's seat of a cross-border evidence gathering operation, guarantees of the traditional mutual legal assistance framework seem to be dropped. A fourth issue is the position of data protection safeguards. US based companies make for significant data suppliers for criminal investigations conducted by EU based authorities. Conflicting legal regimes affect the efficiency of data transfers as well as the protection of personal data to citizens.

[*] Assistant Professor Cyber Security Governance, Institute of Security and Global Affairs, Leiden University.

A. Existing Phenomena and New Questions

There is a new normal in the domain of criminal investigations and that is the growing digital nature of evidence. Whether or not the crime in question is qualified as a computer related crime, a significant part of the material that could be used as evidence can be digital, such as email—messages and their attachments—communication, Facebook profiles, or Whatsapp messages. The fact that citizens are increasingly leaving digital traces while doing everyday acts potentially gives law enforcement authorities an enormous amount of digital data when one or more of these citizens becomes the suspect of a criminal offense. The content of an online shopping cart, the destination of flight tickets booked online, the addressees of email communication, or the GPS coordinates of a recently driven route—as trivial as each of these data points may seem, they can become crucial information for law enforcement officers investigating a specific crime.

In the context of financial crime, an important set of data can be added to this list of examples: Monetary transactions made by the person or persons concerned. The "follow the money" strategy has been labeled as the approach to combat the financing of terrorism and forms of organized crime,[1] but has also been the subject of criticism.[2] Regardless of its effectiveness as a strategy, the gathering of financial data for the purpose of a criminal investigation presents considerable issues concerning data protection and privacy. An individual's monetary transactions show a rather detailed picture of that person's life. Moreover, an individual's bank account and credit card number fall within the scope of the definition of personal data—information that identifies or enables an individual to be identified. The latter means that data protection legislation is applicable to safeguard the data from unlawful or incorrect processing. In the context of a criminal investigation, exceptions to a number of data protection rules are allowed. Data collected for a commercial purpose can be used for a criminal investigation, provided that the data is necessary and proportionate for the investigation and provided that this is laid down in law. The collection of the data for a commercial purpose can be located in a different state than the subsequent use as evidence in a criminal investigation. This cross-border gathering of digital data as evidence is the core topic of this Article. Because the difficulties that are sketched here are related to the digital nature of the data, rather than the type of crime, this Article does not focus on financial transactions, but on personal data as such. More precisely, this paper narrows in on the question of how digital personal data can be accessed and gathered in a cross-border setting in order to produce evidence of (financial) crimes while safeguarding

[1] *See The Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, THE FATF RECOMMENDATIONS (2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

[2] *See* E.W. Kruisbergen, *Combating Organized Crime: A study on undercover policing and the follow-the-money strategy*, 143–45 (2017), https://www.wodc.nl/binaries/Kruisbergen_dissertation_full%20text_tcm28-237785.pdf; *see also* P.E. Neumann, *Don't Follow the Money: The Problem with the War on Terrorist Financing*, FOREIGN AFFAIRS, July/Aug. 2017, at 93–102.

data protection principles. Since this is done from an EU perspective, therefore, this Article's red thread is the cross-border evidence gathering by EU states' law enforcement authorities from US based companies[3] and not vice versa.

There are thus three key phenomena to be joined for the purpose of answering the central question: "Digital personal data," "cross-border criminal investigations," and the "involvement of US based companies as the data supplier." For this analysis it is essential to highlight recent relevant EU legal instruments and proposals: The general data protection regulation[4] ("GDPR"); the directive on data protection for law enforcement purposes[5] ("DDPLE"); the proposed regulation on European production and preservation orders for electronic evidence in criminal matters ("e-evidence regulation"[6]). All three will be the subject of further analysis in this Article.

I. Three Key Phenomena

The three phenomena studied in this Subtitle are not new. All have found their place in the global society for some time. Bringing the three together, however, makes new issues emerge for which a binding legal framework does not yet exist. It is necessary to first reflect on the meaning of these three phenomena separately before examining what such legal framework should look like.

1. Digital Personal Data

The so-called mother convention of data protection—the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data—described personal data as "any information relating to an identified or identifiable

[3] *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*, THE EUROPEAN COMMISSION (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (citing the US as the recipient of the highest volume of requests for digital evidence from EU authorities. Non-paper from the Commission Services).

[4] Commission Regulation 2016/670 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter GDPR].

[5] Directive 2016/680 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 110) [hereinafter DDPLE].

[6] *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 (Apr. 17, 2018) [hereinafter E-Evidence Regulation].

individual."[7] Later, this definition was written into the EU's first legal instrument on data protection: EC Directive 95/46/EC.[8] Thus, it is not necessary to know a person's name or address to identify or single out an individual.[9] Whether the data controller's capability of identifying a person is used or not has little impact on the personal character of the data.[10]

The concept of personal data has been slightly redefined in the aforementioned GDPR and the DDPLE by the addition of a separate definition of "identifiable natural person." The new definition means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name; an identification number; a location; an online identifier; or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[11] An IP address can, for example, qualify as personal data.[12] Even though under the former definition digital personal data were also included,[13] the new definition now explicitly includes digital identifiers.

To illustrate the potential relevance of digital personal data for criminal investigations, it is useful to briefly narrow in on the different types of data—subscriber data, access data, transactional data, and content data—as defined by the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters.[14] Subscriber data pertains to the identity of the user of a service and the type of service, its duration and data related to the validation of the use of service, but not to passwords or authentication means. Access data include the date and time of use of a service—moment of logging in and logging out—and the IP address that is used at that time. Transactional data relate to the transaction of information from a source to its destination and include the sender and recipient of a message, data on the location of the device used, time, duration, size, route,

---

[7] This convention, and the 1980 OECD Guidelines governing the protection of privacy and trans-border flows of personal data, were inspired by two resolutions of the Council of Europe Committee of Ministers—Res 73(22) and Res 74(29)—and a recommendation by the Parliamentary Assembly of 1968.

[8] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

[9] *See* LEE A. BYGRRAVE, DATA PROTECTION LAW, APPROACHING ITS RATIONALE, LOGIC AND LIMITS 43 (2002).

[10] *See id.* at 44.

[11] 2016 O.J. (L 119) 4(1).

[12] Opinion 4/2007 on the Concept of Personal Data, THE WORKING PARTY (2007), https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

[13] Opinion 2/2010 on Online Behavioural Advertising, THE WORKING PARTY (2010), https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf (noting an individual's internet surfing behavior can be so specific that it can qualify as personal data).

[14] *See E-Evidence Regulation*, *supra* note 6 at Art. 2 (7)–(10).

and format. Content data is a residual category made up of all digital data—text, image, video, or audio—that is not subscriber, access, or transactional data. All of the described types of data can encompass personal data and are protected by the EU's data protection provisions, which will be discussed later. The relevance of the distinction described here lies in the amount of protection required. Content data require a stronger protection as they can contain information that is considered to be the private life of one or more individuals. Nevertheless, transactional data are also capable of drawing a detailed picture of an individual's communications: Whom does one communicate with? How often? When? Where does the communication take place? How long does each communication take?[15] Thus, the higher degree of invasiveness of requests for obtaining such data, as compared to subscriber and access data, warrant the distinction made in the European Commission's proposed regulation on digital evidence.[16]

2. Cross-border Criminal Investigations

Criminal investigations that have links to more than one state—due to the location of the perpetrator(s), victim(s), witness(es), or evidence—require mutual legal assistance requests. These requests find their legal basis in a well-established, almost worldwide, framework of multilateral and bilateral agreements. Traditionally,[17] mutual legal assistance requests had to pass through the central authority of the requesting state—usually the ministry of justice—before it could be sent to the central authority of the requested state. The central authority would subsequently forward it to the competent local prosecution or police authority. The 2000 EU Mutual Assistance Agreement[18] introduced direct contact between competent prosecution or police authorities for the first time, but on a wider geographical scale and legal basis—Council of Europe and UN—the traditional sending of requests via the central authority is still the norm. The latter is also the case for the 2003 EU-US Mutual Legal Assistance Agreement[19] and for the 2001 Cybercrime Convention,[20] which contains a significant portion of mutual assistance provisions.

The backbone of the mutual legal assistance mechanism is territorial sovereignty of the states involved. It is thus built on the premise of physical borders defining the territories of

[15] *See* Daniel Solove, *Why Metadata Matters: The NSA and the Future of Privacy*, TEACH PRIVACY (Feb. 12, 2013), https://teachprivacy.com/metadata-matters-nsa-future-privacy/; *see also* Jennifer Daskal, *Law Enforcement Access to Data Across Borders*, 8 J. OF NAT'L SECURITY L. & POL'Y 3, 485 (2016).

[16] *See E-Evidence Regulation*, *supra* note 6; *see infra* Section B.1.

[17] *See* The 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters, E.T.S. No. 30.

[18] 2000 O.J. (C 197).

[19] 2003 O.J. (L 181).

[20] *See* The 2001 Council of Europe Convention on CyberCrime, E.T.S. No. 185.

states and restricting the geographical competence of the authorities involved. When the requested evidence is a tangible object or information of a non-digital nature, such as a paper criminal record or a witness statement, the evidence's location is clear in most circumstances, hence the addressee of a request is also clear. When the requested evidence is digital, such as email communications, however, determining territorial jurisdiction and cross-border evidence gathering becomes a more convoluted process.

3. Involvement of US based Companies[21]as the Data Supplier

Using the traditional mutual legal assistance mechanism for digital data generates a number of requests from competent authorities in all twenty-eight EU member states, most of which are addressed to US authorities.[22] The reason is obvious: Most of the companies we pass our digital personal data to on a daily basis are US based companies.[23] This does not necessarily mean that EU citizens' data will be processed and stored on US territory. Even if they are, that does not mean that they are not protected under the EU data protection legal framework.

With the newly applicable data protection legal framework, companies based outside of the EU that direct their services to EU citizens are required to comply with the provisions of the GDPR. Companies that are data controllers—deciding on the purpose and the means of data processing—as well as companies that are data processors—processing data on behalf of data controllers—are both responsible for compliance with the terms of the GDPR for the specific data processing activities that they conduct. Infringements of GDPR provisions can lead to consequences such as reprimands or suspension of the data processing activities by the supervisory authority or, at worst, it can lead to administrative fines up to twenty million euros or four percent of the total worldwide annual turnover of the preceding fiscal year. Data protection standards such as purpose limitation and data retention are applicable to a US company processing data from EU citizens in the same way they are applicable to an EU company. That should improve the level of protection EU citizens receive, but it is unrelated to the accessibility of the data for EU based law enforcement authorities. The accessibility of the data held by US companies for criminal investigations initiated in the EU is affected by how these companies store their data, however.

---

[21] In order to avoid confusion with the term "service providers," I choose to use the wider term "companies." Companies that offer search engines such as Google are not a service provider in the strict sense of the word because they do not offer Internet access. Search engines, however, collect vast amounts of data that can be requested by law enforcement authorities and should thus be included in this analysis.

[22] *See* IMPROVING CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE, *supra* note 3.

[23] Shobhit Seth, *World's Top 10 Internet Companies*, INVESTOPEDIA (Feb. 16, 2018) https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp (noting that of the top ten of the largest—based on annual revenue—Internet companies in the world, six are American and four are Chinese).

In the following Section, the above three key phenomena will be joined to demonstrate which new questions need to be dealt with in this new normal of borderless digital personal data in a world that is defined by borders.

II. On a Collision Course

When personal data gathered, processed, and stored by US based companies is needed for the purpose of a criminal investigation in the EU, how does the digital nature of those data change the mechanism? In this subtitle we look at the borderless digital storage practices of companies and how states have created different ways to obtain data needed for criminal investigations.

1. Digital Storage

Companies often use cloud storage for securely storing their data. Essentially, cloud storage means storage of data on one or more servers possibly owned by someone else rather than storage on one's own computer hard drive or portable device. Companies either have their own cloud or rent cloud storage space from another company: A cloud provider. The use of cloud storage affects the search for data by law enforcement authorities in two ways. First, the server does not need to be physically located at the premises of the cloud provider. It can even be located in a different country. Creating physical distance between administrative offices and data locations can be beneficial from a security point of view or it can be done for legal reasons—for example, a more lenient data protection regime. Second, many companies buy or rent cloud storage from cloud providers, not necessarily knowing where exactly these companies have built their servers—or data centers—or in which data center their data are located at any given moment. To secure the data stored in these centers, companies can distribute the data across servers in different locations. The data is then cut up in parts and replicated over multiple systems while the company tracks the location and status of each hard drive of their data centers.[24] Furthermore, the distribution of data over servers can change automatically depending on how the company has organized its data centers. Such a practice is used by Google "as frequently as needed to optimize for performance, reliability and other efficiencies," and led the ubiquitous company to declare in a recent court case that, at the time of an authority's request for data, the location of the data can be different from the location at the time the request is executed.[25]

Following the logic of the GDPR, a data center in itself would not qualify as the main establishment of a company. To qualify the data center would need an effective and real exercise of management activities—through stable arrangements—which determine the

[24] *See Data and Security,* GOOGLE https://www.google.com/about/datacenters/inside/locations/index.html.

[25] *In re* Search Warrant No. 16-960-M-01 to Google (E.D. Pa. 2017).

main decisions as to the purposes and means of the data processing.[26] Both situations described above can still lead to issues when the digital data in question are being moved to be stored in a data center of the company located in a third state whereas that company has a main establishment in the EU. For example, if Google has its main EU establishment in Ireland but the data wanted for a criminal investigation conducted by Spain are stored on a server in Brazil, in case of the automatic "data hopping," the data could be stored within yet a different jurisdiction at the time the Brazilian authorities would execute the request.

2. Law Enforcement Requests for Digital Data

To use the term accurately developed by Jennifer Daskal, data is infamously un-territorial,[27] especially when the above-described dynamic distribution of data or data hopping is taking place. What does this mean for criminal investigations and prosecutions? The question is particularly significant considering that criminal procedure laws are typically national laws. Thus, the legal framework governing data gathering for the purpose of investigating and prosecuting criminal offenses is territorial whereas the data themselves are not. This collision between territorial laws and un-territorial data presents two legal questions.

The first question is whether mutual legal assistance in criminal matters is a mechanism that functions when cross-border digital evidence is concerned? Traditionally, law enforcement authorities request cross-border evidence in the EU-US relations by using mutual legal assistance requests. Yet these requests are addressed to the authorities of the requested state, not the companies holding the data. Multilateral mutual legal assistance treaties do not provide indirect contact between law enforcement authorities of one country and a private company of another country. Inherently request-based, the system of mutual legal assistance is also notoriously slow. With time being an essential element in criminal investigations, especially when easily moved digital evidence is concerned, corrupted or destroyed, a number of EU member states have turned to sending direct requests for digital data to companies in third states.[28] When companies are located in a third state, a conflict of laws may arise if their national law does not allow for handing over the data.

Practice among EU member states demonstrates the relevance of questioning traditional mutual assistance. When the European Commission services distributed a questionnaire[29] among the EU member states in 2016 aiming to gain insight in how member states handled

[26] *See* GDPR, *supra* note 4 at recital 36 of the preamble.

[27] Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L. J. 326, 326–98, (2015).

[28] *See* IMPROVING CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE, *supra* note 3; *see also Questionnaire on Improving Criminal Justice in Cyberspace*, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

[29] *See Questionnaire*, *supra* note 28.

cross-border access to digital evidence, the result revealed a surprisingly diverse patchwork of terminology used as well as approaches to obtaining the evidence.[30]

At the time of the questionnaire, the European Investigation Order had not been implemented, so member states' authorities should have relied on either the unpopular European Evidence Warrant or the aforementioned EU mutual legal assistance agreement. Nonetheless, in those cases where a company was located outside the domestic jurisdiction—but still in the EU—twenty-four out of the twenty-seven member-states that replied to the questionnaire relied on sending direct requests by national authorities to companies in another member state. Of those twenty-four, seventeen member-states consider these direct requests voluntary, and seven consider them mandatory. Only three member-states indicated having specific legislation for this type of cooperation. No less than twenty-four member-states do not allow companies established on their territory to respond to direct requests from authorities in other member states or do not provide for this in their national laws.

The picture is slightly different when the wanted data should be obtained from a company based in a third state. In this context, and given that the location of the data is known, the instrument to use is clear. Mutual legal assistance requests are the only option. Mandatory orders for data outside the framework of a bilateral or multilateral agreement would most likely be considered a serious breach of the sovereignty of the third state in question. Nevertheless, the mechanism of mutual legal assistance in criminal matters is not unproblematic. A concern that is not new in this context is the time-consuming nature of mutual legal assistance requests. It is a complaint that has been haunting mutual legal assistance procedures for decades. Other concerns are related to the digital nature of the evidence such as the use of mutual legal assistance procedures for access to information where under US law no mutual legal assistance request is required—such as subscriber data, or the difficulty to establish probable cause and the lack of dual criminality. When the location of the data is unknown, member states responded to the questionnaire with a variety of approaches. Aiming to find out the location of wanted data, multiple mutual legal assistance requests could be used, but are a rather inefficient and time-consuming method. Five member-states indicated that their competent authorities could directly access digital evidence when the location is unclear or when it is impossible to establish its location. Fourteen member-states indicated that this depends on specific circumstances. Such method of working could entail significant sovereignty issues on the part of the third state.

The second question relates to the data storage practices described above. When companies store data or data parts on servers in different locations, what is the determining factor for

[30] *Measures to improve cross-border access to electronic evidence for criminal investigations following the conclusions of the Council of the European Union on improving criminal justice in cyberspace* (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf.

deciding where to send the request for data: The main establishment of the company, or the physical location of the data? A similar question—although in the opposite direction, from a US authority requesting EU based data—was raised in the Microsoft Ireland case when Microsoft refused to comply with a warrant from US authorities to hand over data on an email account that were stored on a server in their Irish data center.[31] The question was not whether the national law applied outside the territory of the US—the parties agreed that it does not—rather, the question was whether data stored on a server in Ireland, controlled by a US based company, were located in Ireland or in the US? The answer would determine whether a mutual legal assistance request was needed, or whether it was a purely domestic request for data. The difference between both options in terms of jurisdiction, grounds for refusal of the request, and time spent are considerable. In the meantime, the case before the Supreme Court was declared moot due to the adoption of a new law by the US Congress in March 2018.[32] The so-called CLOUD Act as well as its EU counterpart will form the heart of the following subtitle.

A. Defensive Cooperation Avoiding Collisions

Both the EU and the US have recently initiated legislative solutions to improve access to digital data for the purpose of criminal investigations. The US Clarifying Lawful Overseas Use of Data or CLOUD Act was not the subject of elaborate discussion in Congress, but buried in more than 2,000 pages of a spending bill adopted on March 23, 2018. Even though the European Commission already started preparations on its own proposed legislation to regulate cross-border electronic evidence in 2016, European Justice Commissioner Jourova expressed her disappointment that the CLOUD Act's swift adoption did not allow for a compatible solution between the EU and the US.[33]

I. Proposed European Preservation and Production Order

On April 17, 2018, the European Commission presented its proposals for electronic evidence in criminal matters, the so-called e-evidence proposals. Inspired by the results of the aforementioned questionnaire, the European Commission developed several non-legislative and legislative options to rectify the situation and offer member states legal certainty on what to do when digital data is needed from a company based in a third country. The

[31] U.S. v. Microsoft, 584 U.S. 1 (2018) (per curium).

[32] CLOUD Act, H.R. 4943, 115th Cong. (2018).

[33] Nikolaj Nielsen, *Rushed US Cloud Act Triggers EU Backlash*, EUOBSERVER (Mar. 26, 2018), https://euobserver.com/justice/141446.

proposed approach is a regulation introducing a preservation and production order,[34] and a directive on how companies should select their legal representation in the EU.[35]

The European preservation and production orders are developed from the same line of reasoning as the existing mutual recognition measures. The strongest similarities exist with the freezing order and the confiscation order—now replaced by the European Investigation Order.[36] The freezing and confiscation orders could equally be used in a successive order. Whereas the freezing order ensured the immobilizing of evidence awaiting a subsequent confiscation order, the preservation order secures the wanted data in view of a subsequent order to produce the data. If no concern that the data would be deleted, moved, or otherwise modified is presented, the production order could also be used as a stand-alone measure. A European Investigation Order or a mutual legal assistance request could also follow up preservation orders.

An important characteristic of the proposed regulation that sets it apart from previous mutual recognition instruments is its significant effect on third states. The scope of the proposed regulation reaches beyond the borders of the EU, as it includes companies that provide services in the EU. Resembling the scope of the GDPR to some extent, the Commission is hereby responding to a highly digitalized world governed by companies based outside the EU. Offering its law enforcement and judicial apparatus the proper tools to work with, the Commission accompanied this wide scope of the proposed regulation with a directive that obliges all service providers operating within the EU to appoint a legal representative within the EU. This will allow the competent authority of an EU member-state wanting to obtain digital data from a US based company such as Facebook, to contact their legal representation in the EU—most likely the Dublin office—through a preservation or production order rather than by sending a mutual legal assistance request to the US central authorities.

The scope of the proposed regulation is limited to data stored at the time of receipt of the order. Real-time interception of telecommunication is thus excluded and will remain to fall within the scope of the European Investigation Order or the EU mutual legal assistance agreement. Based on the level of intrusiveness, the proposed regulation distinguishes two classes of digital data. As explained under Subtitle I.1., subscriber and access data are considered to be less sensitive in comparison to transactional and content data, bringing the latter two under a more protective regime. For obtaining transactional or content data, the

[34] *See E-Evidence Regulation*, *supra* note 6.

[35] *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*, COM (2018) 226 final (Apr. 17, 2018).

[36] Denmark and Ireland are not taking part in the European Investigation Order so for cooperation with these member states, the freezing and confiscation orders can still be used.

production order should be issued by a judge, a court, or an investigative judge. Prosecutors can only issue production orders for subscriber or access data. Moreover, production orders for transactional or content data may only be issued for the more serious of offenses.[37] The distinction in types of data only applies to production orders, not to preservation orders.

The real innovation in the proposed regulation—and the similarity with the US CLOUD Act—is the recognition of potential conflicts of laws affecting the companies involved. When a company based outside the EU offering services to EU citizens receives a production order from an EU member-state's authority, it is likely that the company is prohibited by its own national law to transfer the data—for example, the US Electronic Communications Privacy Act.[38] Such situations created legal uncertainty for the company but also created a waste of time and resources since the issuing authority had to subsequently rely on other channels to obtain the evidence needed for a running criminal investigation. To solve this unsatisfying situation, the proposed regulation introduces a right for the companies in question to raise a reasoned objection to the production order and have the case reviewed by a court—of the member state involved—if the issuing authority insists on upholding the order. When the court determines that there is a conflict of laws, an opinion should be requested of the third state. Only if the third state's laws aim to protect fundamental rights of citizens or fundamental interests related to national security or defense, the production order must be withdrawn. In the opposite case, the court should balance the interests at stake.

This is different reasoning from the traditional mutual legal assistance mechanism. The latter is based on issuing a request to a state's central authority—usually the ministry of justice—and having this authority assess whether fundamental interests of the requested state or of individuals involved should be protected before confirming or denying the execution of the request. Whether or not such assessment takes place in the context of the production order now lays in the hands of a company rather than a ministry of justice. This raises the issue of whether a company is in the right position to make such assessment. Companies' main interest is doing business and making money. Delivering data to states' competent authorities is not part of that. This does not mean companies do not want to be compliant; they are simply not equipped to handle mutual legal assistance related questions. Imagine if a company that receives a request for data does not see a conflict of law and transfers the requested data to the requesting state. After the transfer, the national authorities of the company's main seat see the transfer as a violation of their national laws. Does that make the evidence delivered to the requesting state inadmissible? Could a company be held liable for such conduct and the consequences thereof for a running criminal procedure? These are once again new questions that are, so far, unanswered.

---

[37] *See E-Evidence Regulation*, *supra* note 6 at Art. 4 (defining criminal offenses punishable in the issuing state by a custodial sentence of a maximum of at least 3 years or fraudulent money transfers, offenses related to sexual abuse and exploitation of children and terrorism offenses wholly or partly committed by means of an information system).

[38] *See infra* Section B.2.

A substantial improvement in the mechanism of cross-border evidence gathering introduced by the proposed regulation is the speed with which preservation and production orders should be executed. Preservation orders should be carried out without undue delay. Production orders should result in a transfer of the wanted data within ten days upon receipt of the order unless valid reasons are given for non-compliance. In cases of an imminent threat to life or physical integrity of a person or to a critical infrastructure, the deadline is shortened to six hours. In comparison to the 120 days for obtaining data via a European Investigation Order or the average ten months for receiving data resulting from a mutual legal assistance request,[39] the shorter deadlines are appropriate for the fast-paced character of digital evidence. Still, if the proposed regulation is adopted in an unchanged format, companies will be forced to invest considerable resources in preparing for a number of production orders that have to first be studied for potential conflict of laws and then be either objected to or complied with.

II. US CLOUD Act and Privacy Shield

The proposed EU regulation on preservation and production orders was partially inspired by the conflict of laws created by the US Electronic Communications Privacy Act ("ECPA".) The ECPA blocked disclosure of content data in most circumstances of requested cross-border transfer. In March 2018, against the background of a data sharing agreement between the US and the UK,[40] the ECPA was amended by a new act. This new act, appropriately named the CLOUD Act,[41] allows US based companies to hand over data regardless of the physical location of the data, under the condition that it does not concern data about US persons or residents. EU member states' competent authorities could thus benefit from the CLOUD Act so long as they do not need data on American citizens or residents. The requesting state, however, needs to meet a high standard of substantive and procedural protections for privacy and civil liberties.[42]

[39] *New EU Rules to Obtain Electronic* Evidence, EUROPEAN COMMISSION (Apr. 17, 2018), http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

[40] Madhumita Murgia, *UK-US pact will force big tech companies to hand over data*, FINANCIAL TIMES (Oct. 23, 2017), https://www.ft.com/content/880bc2ae-b980-11e7-9bfb-4a9c83ffa852.

[41] CLOUD Act, H.R. 4943, 115th Cong. (2018).

[42] Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018), https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

An additional agreement with the US is still necessary in accordance with article 48 of the GDPR[43] that only allows personal data transfers with a legal basis in mutual legal assistance agreements or other international agreements.[44] The EU-US mutual legal assistance agreement of 2003—applied in relation to the prior existing bilateral mutual legal assistance agreements between EU member states and the US—would not qualify as the agreement that brings the CLOUD Act in line with the GDPR because it is applicable to states exchanging data and not a state's authorities requesting a company directly for data. Moreover, the provisions of article 9 of the 2003 EU-US agreement on limitations on use of personal and other data are formulated to favor less restriction on the use of data by requesting EU or US authorities over more restriction;[45] something that is not the tone of the CLOUD Act, considering the list of factors to be fulfilled before a foreign government could receive data from a US based company. These factors include adequate substantive and procedural laws on cybercrime and electronic evidence, demonstrated respect for the rule of law and principles of non-discrimination and adherence to international human rights obligations. Formally recognizing EU member-states as fulfilling these factors would significantly improve EU-US cooperation in criminal matters.

The list of factors to be fulfilled by a non-US government prior to receiving data from a US based company reminds us of the adequacy requirement introduced in the aforementioned EC Directive 95/46/EC in the other direction, namely imposed by the EU onto third states such as the US. The EU was the first to demand a certain level of data protection in a third state as a prerequisite to that state processing any EU-originated personal data. US academics did not welcome this requirement,[46] not in the least due to the substantial differences between the EU and the US data protection legal frameworks. The disagreements made approval of the US' data protection regime as adequate doubtful. These differences were largely ironed out by the Safe Harbor agreement, replaced with the EU-US Privacy Shield.[47]

---

[43] *See* Amicus Curiae Brief of the European Commission on Behalf of the EU in the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation, U.S. v. Microsoft, 584 U.S. 1 (2018) (per curium).

[44] *See* Christin McMeley & John Seiver, *The CLOUD Act — A needed fix for US and foreign law enforcement or threat to civil liberties?* IAPP (Feb. 28, 2018), https://iapp.org/news/a/the-cloud-act-a-needed-fix-for-u-s-and-foreign-law-enforcement-or-threat-to-civil-liberties/.

[45] *See* ELS DE BUSSER, DATA PROTECTION IN EU AND US CRIMINAL COOPERATION: A SUBSTANTIVE LAW APPROACH TO THE EU INTERNAL AND TRANSATLANTIC COOPERATION IN CRIMINAL MATTERS BETWEEN JUDICIAL AND LAW ENFORCEMENT AUTHORITIES, 353–54 (2009).

[46] *See* George B. Trubow, *European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flows* 13 NE. J. OF INT'L L. & BUS., 176 (1992–1993); *see also* William J. Long & Marc Pang Quek, *Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, 9 J. OF EUR. PUB. POL'Y 325, 326 (2002).

[47] Commission Implementing Decision (EU) 2016/1250 of July 12, 2016 pursuant to the Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-US Privacy Shield,

In spite of the earlier critiques from US scholars on the EU adequacy requirement, the US CLOUD Act equally includes a set of prerequisites the recipient state should fulfill before a data transfer can take place. This is not the first time that a US law provides a copy of the adequacy requirement. In the Judicial Redress Act[48] we see a clear set of conditions imposed on states wishing to benefit from the expanded redress rights. The Judicial Redress Act is a law adopted after pressure from the European Commission on the US government to grant EU citizens judicial redress for unlawful processing of personal data under the 1974 US Privacy Act.[49] Pressure to adopt the law increased after both parties agreed to sign the so-called EU-US Umbrella Agreement, a pact that can be best described as a "superstructure" added to earlier concluded EU-US agreements consisting of safeguards protecting data exchanged under the terms of the agreements.[50]

III. The Effect on Data Protection

Both the EU and the US impose an a priori requirement on the recipient state's level of respect for certain rights, which adds a new dimension to cross-border data exchanges. When personal data leaves the EU to be processed in the US, the US' level of data protection should be adequate, which includes inter alia adherence to human rights. In cases where data transfers in both directions are made for law enforcement purposes, the EU-US umbrella agreement and the EU-US mutual legal assistance agreement ensure additional safeguards. When EU authorities want to receive digital data directly from a US based company, they need to show respect for the rule of law, adequate laws on electronic evidence and cybercrime, and compliance with human rights. As argued above, an additional agreement is still needed because the data transferring party is a company and not an authority.

In spite of this list of existing agreements and one future agreement, we effectively see here the imposing of rules on other states by introducing national laws rather than international

2016 O.J. (L 207) (Both the Safe Harbor agreement and the Privacy Shield are based on the same mechanism: a set of data protection principles signed by a long list of US based companies committing themselves to compliance with these principles. Since the Safe Harbor agreement was annulled due to insufficient necessity and proportionality safeguards and lacking redress for EU citizens (Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650), the Privacy Shield enhances data protection.

[48] The Judicial Redress Act of 2015, H.R. 1428, 144th Cong. (2016).

[49] *See Big Data: A Twenty-First Century Arms Race*, ATLANTIC COUNCIL (2017), http://www.atlanticcouncil.org/images/publications/Big_Data_A_Twenty-First_Century_Arms_Race_web_0627.pdf.

[50] *Id.*

agreements.[51] The adequacy requirement of Directive 95/46/EC was an example, its successor, the GDPR, follows suit. Now the US Cloud Act has a similar effect. It is not unthinkable that the GDPR's wide scope could lead to an export of EU data protection standards as US-based companies may have a hard time distinguishing between their data processing of EU customers data and non-EU customers data and will thus apply the EU standards to all their data processing activities. Ultimately, we may see data localization and market segmentation as potential consequences.[52] This norm creation without international agreements fits in the departing from traditional mutual legal assistance in criminal matters.

B. The Fast Track

Not that long ago, the European Investigation Order was considered the fastest tool in the hands of competent EU authorities to obtain information and material in the context of a cross-border criminal investigation. Aiming to speed up the notoriously slow mutual legal assistance process, limit grounds for refusal, shorten deadlines, and standardize forms created a mechanism for conducting most cross-border investigative measures between EU member states. The European Investigation Order has only been applicable for a little more than a year now; still, it is already considered too slow for digital evidence.

Even though mutual legal assistance and the European Investigation Order will remain in place, the new proposed regulation introducing preservation and production orders for digital data resembles the fast-track line at the security control section of an airport. This race to develop speedier cross-border cooperation tools is triggered by the fast-paced digital society we live in today. Mutual legal assistance procedures that make requests move between central authorities of the requesting and requested state before reaching the locally competent (judicial) authority have no place in today's digital society. Yet, that does not necessarily mean that a new mechanism should be introduced which makes a company the requested party rather than a state's central authority or competent authority.

Besides the significant investment that is expected from companies to assess every incoming production order to potential conflicting laws, the proposed regulation puts companies in a position they should not be in: The position of protecting the sovereignty of the state where they have their main seat. In fact, the ties between that particular state—whose laws allowed the company to be founded in the first place—and the physical location of digital data stored by the company are cut. When Google stores data in a data center in Brazil, a German judge can have them produced by addressing the EU legal representation of Google. The only way the Brazilian law could put a stop to it is if it would create a conflict of law that should be flagged by Google.

---

[51] Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9 (2018) (referencing to Anu Bradford, *The Brussels Effect*).

[52] *Id.*

Mutual legal assistance was developed in a slow-pace manner due to the assessment it allowed the requested state to make. That state had the chance to perform a thorough check of the compatibility of the requested investigative measure with its own sovereignty, security, or essential interests. It enabled a state to, for example, refuse cooperation to possible political prosecution in the requesting state. Even in the EU's area of freedom, security, and justice where mutual trust should theoretically exist, based on which mutual recognition should limit the grounds for refusal to cooperate more, a real risk for violation of the individual's fundamental rights was recognized as a valid reason to refuse cooperation.[53] Moving away from mutual legal assistance to make room for faster cooperation should be a beneficial development. One that is necessary considering the amount of digital evidence. It is not a beneficial development when guarantees protecting states' sovereignty and individuals' rights are left as well.

[53] *See Joined Cases C-404/15 & C-659/15 PPU Pál Aranyosi & Robert Căldăraru* (Apr. 5, 2016) http://curia.europa.eu/juris/liste.jsf?num=C-404/15.