3

The Commission's E-Evidence Initiative: Harmonising EU Rules on Access to Electronic Evidence

LANI COSSETTE*

I. Introduction

In today's plugged in, always-on world, it is worth pausing to reflect just how dramatically things have changed in the last 25 years. When I started my career as a journalist two and a half decades ago, I filed my stories on the only computer in the office using a beta version of Mosaic and an email account from AOL. Some of my colleagues filed their stories using a word processor. We made interview requests using a fax machine, or even by regular post. And when we needed to store documents, we sometimes printed documents and stored them in manila files. I had a manila file labelled 'Internet' and a phone book for the 'world-wide-web' on my bookshelf.

Compare that to where we are today. Webmail, texting, instant messaging, social media, web-based videoconferencing – the ways we communicate are remarkably diverse and continually expanding. We create more content than ever before, in more creative ways than ever (using text, videos, photos, graphics, even emoji), and often are happy to have this information exist only in digital form. We might hold some of this content on our devices, but much of it exists solely in the cloud – with the electronic bits sometimes stored in a different country, or on services operated by providers in foreign jurisdictions.

It is hard to overstate the impact of this shift to the world of online services. These services are bringing people together and changing the way we work in significant ways, providing new opportunities to share information, to collaborate with colleagues, and to join and build communities. Through the magic of search, billions of people across the planet now have more information at their fingertips

* Lani Cossette was a Director for EU Government Affairs at Microsoft and currently Senior Director and Chief of Staff, UN Affairs at Microsoft. All views expressed herein are her own and do not necessarily reflect the views of Microsoft.

than could fit in the world's greatest libraries combined. They are also transforming the economy, making companies more efficient, bringing them closer to their customers and partners, and opening whole new markets and new avenues to innovate.

However, consumers and businesses are not the only ones going online. The Internet has also become a means through which criminals plan or execute their crimes, and where crucial information about criminal activity may be stored. This means that law enforcement authorities often find that the evidence they need to solve or even prevent crimes exists only online. However, since many online services store users' content and other information 'in the cloud' (that is, in remote data centres), it is increasingly likely that the place where evidence of a crime is located, or where the entity holding that evidence is established, is subject to different laws to those prevailing where the crime occurred. Although that can create challenges for law enforcement, it also raises issues that are of fundamental importance for people and society. For instance, how do we best balance the public's interest in law enforcement against the individual's right to privacy? How should we resolve the conflicts that arise when compliance with an order to disclose evidence in one country violates the laws of another? To what extent should providers of services that people use to store personal information or handle confidential communications have the ability to defend the interests of their users in the face of demands from the state to disclose this information? These are difficult questions, in part because they impact many different stakeholders, but also because they often implicate laws, norms and values in multiple jurisdictions. This is especially true in the European Union, given the close economic and social integration of multiple sovereign Member States.

II. The Challenge

The growing use of online services means that criminal activity today is far more likely to have a cross-border dimension than ever before. Consider, for example, the scenario of a German lawyer accused of stealing funds from a French victim. Assume the lawyer is suspected of having conspired with a client to commit the crime using email, and that the emails reflecting this conspiracy are now stored in a data centre located in Sweden, operated by a service provider based in the United States and whose only European office is in Ireland. What happens when French authorities seek access to these emails? In order to avoid alerting the suspect of the investigation, French authorities might want the service provider to disclose the emails. Given that the provider is based in the United States and has its only European office in Ireland, however, any demand served directly on the provider could intrude on US and/or Irish sovereignty and might conflict with legal obligations arising under their laws. And what if the emails are protected by German data-protection or privacy laws, or German law protecting client confidentiality?

Should German authorities have a say in whether the emails are disclosed? What about Sweden, where the emails are physically stored?

Although law enforcement authorities need clear answers to these questions, *how* we answer them matters to all of us. Most people, for instance, consider privacy to be a fundamental human right, and few would expect this right to be checked at the door when they go online. Also, people expect that the law where they live should apply and that they should not be subject to conflicting legal obligations. Where such conflicts do arise, most people would expect the respective governments to resolve them. Policymakers across the globe are working to address these issues in ways that appropriately consider privacy and security interests in our increasingly borderless world.[1] Parties to the Council of Europe Convention on Cybercrime, for instance, are considering a protocol to the Convention that would facilitate the ability of law enforcement in one jurisdiction to serve orders directly on providers in another.[2] As explained by Giuliani in the following chapter, in the United States, lawmakers recently adopted the CLOUD Act, which authorises US law enforcement to obtain data from service providers subject to US jurisdiction, regardless of where the data is stored, but also authorises the US Department of Justice to negotiate agreements with foreign governments to remove legal restrictions on the ability of providers to disclose data directly to authorities of the other party.[3] Although these initiatives take different approaches, each seeks to address the increasingly cross-border dimensions of crime in ways that respect basic notions of privacy and sovereignty while minimising conflicts of law.

III. The EU's Proposed Solution: The E-Evidence Package

The Commission offered its own potential solution to these issues in April 2018 when it published the proposed EU Electronic Evidence (e-evidence) legislative package.[4] The Commission recognised that various EU Member States were taking divergent approaches to obtaining evidence in criminal investigations having

[1] Brad Smith, 'A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data' (*Microsoft Corporation*, 11 September 2018) blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/.

[2] Council of Europe, 'Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime' (June 2017) rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b.

[3] Congress enacted the CLOUD Act as part of the 2018 Consolidated Appropriations Act, PL 115–41. The full text of the CLOUD Act may be found at: www.justice.gov/dag/page/file/1152896/download, accessed 31 May 2020/. For an analysis, see ch 4 in this volume.

[4] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM(2018) 225 final (Proposal for an E-Evidence Regulation); Commission, 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' COM(2018) 226 final (Proposal for an E-Evidence Directive).

cross-border dimensions (for example, where the evidence or provider was located in a different jurisdiction) and that the lack of coordination at the EU level was creating barriers to the Single Market. As the Commission explained:

> [T]his proposal aims to remove some of the obstacles to addressing the service providers by offering a common, EU-wide solution for addressing legal orders to service providers. …
>
> [This] harmonised approach creates a level playing field for all companies offering the same type of services in the EU, regardless of where they are established or act from.

Harmonised rules at EU level are not only necessary to eliminate obstacles to the provision of services and to ensure a better functioning of the internal market, but also to ensure a more coherent approach to criminal law in the European Union. Furthermore, a level playing field is necessary for other fundamental premises for the good functioning of the internal market, such as the protection of fundamental rights of citizens and the respect of sovereignty and public authority when it comes to the effective implementation and enforcement of national and European legislation.

The e-evidence package consists of two proposed legislative instruments: a Directive[5] and a Regulation.[6] The Directive would require online service providers that either are established in, or have a 'substantial connection' to, the European Union to appoint a legal representative in at least one Member State.[7] Service providers would need to empower their representative to receive and comply with orders to produce evidence in criminal matters from authorities in *any* Member State.[8] If the representative refuses or is incapable of complying, both the provider and its representative could be sanctioned.[9] In effect, the Directive creates a 'one-stop shop' for authorities in every Member State to obtain criminal evidence from any service provider offering services in the EU.[10] Critically, legal representatives must comply with orders regardless of where the crime took place, where the provider is established, or where the evidence is stored, and irrespective of the nationality or residence of the target – even if any (or all) of these locations are outside the EU. In that sense, the Directive has clear extraterritorial reach. While the Directive requires service providers to appoint a legal representative that has the ability to *comply* with orders for evidence in criminal investigations, it does not

[5] See n 4.

[6] ibid.

[7] The proposal for an E-Evidence Directive states that the substantial connection criterion 'should be assessed on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States'. See recital 13. The Directive would not apply to service providers established and offering services in a single Member State. See Directive, Art 1(4).

[8] Proposal for an E-Evidence Directive, Art 3.

[9] ibid Art 5.

[10] Service providers are free to appoint legal representatives in more than one Member State if they wish. See Proposal for an E-Evidence Directive, Art 3(4).

provide an independent legal basis for authorities to *issue* such orders. For that, authorities must rely on a separate domestic or EU legal measure that empowers them to compel such disclosure. The E-Evidence Regulation would establish two such measures at EU level: (i) European Production Orders (EPOs), which Member State authorities could issue on a service provider established, or with a legal representative, in a different Member State, requiring the provider to *disclose* evidence;[11] and (ii) European Preservation Orders (EPrO), which likewise could be issued on providers established or legally represented in a different Member State, but only requiring providers to *preserve* evidence (which authorities would then obtain pursuant to a separate instrument).[12] Although authorities could use EPOs to obtain all types of data, EPOs for more sensitive data, for example for the content of an email, or revealing identity of the sender or recipient,[13] would be subject to various protections, for instance that they could be used only in relation to serious crimes.[14] As with the Directive, Member State authorities could use EPOs and EPrOs to compel service providers to disclose or preserve evidence (respectively) regardless of where the crime took place, where the provider is established or where the evidence is stored, and irrespective of the nationality or residence of the target. Here again, the Regulation in these respects would have clear extraterritorial effects. However, where a provider believes that compliance with an EPO would require it to violate the laws of a third country, the Regulation would require judicial authorities in the issuing Member State to address that conflict. If these authorities determined that compliance would conflict with a third-country law that 'is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence',[15] they would provide relevant information about the order to authorities in that third country. If those third-country authorities objected to the disclosure, the issuing Member State's judicial authority would have to deny the order. If the third-country authorities did not object (or failed to respond within a certain period), the judicial authority would uphold the order – even if this compelled the service provider to violate the third country's laws.

IV. Potential Reforms to the E-Evidence Regulation

As a leading provider of online services, Microsoft welcomes efforts by governments to harmonise rules governing law-enforcement access to electronic data, both to ensure that authorities can access the data they need to keep

[11] Proposal for an E-Evidence Regulation, Art 5.
[12] ibid Art 6.
[13] ibid Art 2(9), defining 'transactional data', and Art 2(10), defining 'content data'.
[14] ibid Art 5(4).
[15] ibid Art 15(1).

people safe and to ensure that user and customer rights are fully respected. Although Microsoft recognises that authorities often need to obtain data held by service providers in order to solve crimes and protect the public, we also believe that the rules governing access to this data should respect the fundamental rights of users and appropriately address potential conflicts of law. To this end, Microsoft has articulated six principles to help guide policymaking in this area:[16]

1. *Universal right to notice:* Absent narrow circumstances, users have a right to know when the government accesses their data, and cloud providers must have a right to tell them. …
2. *Prior independent judicial authorisation and required minimum showing:* Law enforcement demands for content and other sensitive user data must be reviewed and approved by an independent judicial authority prior to enforcement of the order, and only after a meaningful minimum legal and factual showing. …
3. *Specific and complete legal process and clear grounds to challenge:* Cloud providers must receive detailed legal process from law enforcement to allow for thorough review of the demand for user data, and must also have clear mechanisms to challenge unlawful and inappropriate demands for user data to protect human rights. …
4. *Mechanisms to resolve and raise conflicts with third-country laws:* International agreements must avoid conflicts of law with third countries and include mechanisms to resolve conflicts in case they do arise. …
5. *Modernising rules for seeking enterprise data:* Where an enterprise stores data with a third-party service provider, the enterprise should retain the right to control that data and should receive law enforcement requests directly. …
6. *Transparency:* The public has a right to know how and when governments seek access to digital evidence, and about the protections that apply to their data.

The Proposal for an E-Evidence Regulation reflects several of these principles. For example, where a law enforcement agency seeks data that a cloud provider stores on behalf of an enterprise, the proposal states that they should first seek the data from the enterprise itself unless doing so would jeopardise the investigation.[17] The proposal also requires that EPOs for user content and similarly sensitive data must be issued or validated by an independent judicial authority.[18] In other respects, however, the Regulation, including the amended text endorsed by the Council of the EU on 12 December 2018 ('the Council general approach'), could benefit from further changes.[19] In particular, the current versions under discussion do not fully resolve the conflicts of law and intrusions on sovereignty that

[16] 'Six Principles for International Agreements Governing Law-Enforcement Access to Data' (*Microsoft*) blogs.microsoft.com/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf.

[17] Proposal for an E-Evidence Regulation, Art 5(6).

[18] ibid Art 4(2).

[19] Council of the European Union, Document 15292/2018 (12 December 2018).

inevitably arise with law enforcement demands that have cross-border dimensions; they also put fundamental rights at risk. To address these concerns, our suggestions are as follows:

A. Stronger Rights of Notice for People Targeted by Orders

People have a right to know when governments access their data. Without notice, data subjects may find it more difficult to exercise their fundamental rights to privacy and to judicial redress.[20] In some cases, providing such notice will be problematic, for instance if it could imperil an ongoing investigation or create a risk to public safety. In those circumstances, however, law enforcement should be required to obtain a non-disclosure order (NDO) from an independent judicial authority based on a factual showing both that secrecy is necessary and that prohibiting the service provider from providing such notice is needed to prevent further harm. Any such NDO should be narrowly tailored in duration and scope and should allow providers to challenge the order on grounds of overbreadth. The proposed Regulation achieves none of these goals. In fact, Article 11 of the Council text would *prohibit* service providers from notifying customers about orders seeking their data (unless the issuing authority explicitly requests the provider to provide such notice). The Council text also imposes no obligation on law-enforcement authorities to prove their need for an NDO to an independent judicial authority, or to establish that these restrictions on notice are no broader than necessary and respect the fundamental rights of affected parties.[21] In order to achieve a more appropriate balance between the needs of law enforcement and the rights of users, service providers should be enabled to notify users of any EPO seeking access to their data *unless* the order is accompanied by a separate NDO prohibiting such notice. To obtain an NDO, law enforcement should have to establish, before an independent judicial authority, that providing such notice would imperil an ongoing investigation or endanger public security, and that the order is limited in scope and duration to what is necessary and proportionate.

B. Meaningful Notice to Affected Member States

In some cases, information sought by an EPO might be eligible for privileges or immunities granted by the laws of the Member State where the target or other affected people reside. For instance, recall the earlier hypothetical involving an

[20] See Charter of Fundamental Rights of the European Union, Art 7 (right to respect for private and family life) and Art 47 (right to an effective remedy and to a fair trial).

[21] Although the Council text states that issuing authorities shall notify the person whose data is sought, they may delay doing so 'as long as it constitutes a necessary and proportionate measure'. See Council Document 15292/18 (n 20).

alleged conspiracy between a German lawyer and its client: their email communications might be protected by German laws on lawyer–client privilege, and Germany might wish to ensure that the suspect retains its right to preserve this privilege in the face of demands from French authorities seeking these communications. However, in its current wording, the proposed Regulation would not require French authorities to notify German authorities about the EPO, nor would it give them a basis to object. The Commission proposal does not address this issue at all. The Council general approach merely states that, in cases where the issuing authority has reasonable grounds to believe that an EPO seeks data of a person who is not residing on its own territory, it must send a copy of the order to the *enforcing* Member State (that is, the Member State where the service provider receiving the order is established or has its legal representative).[22] Neither the Commission nor the Council text requires any form of notice to the Member State where the target lives (for example, the 'affected' Member State).

This approach makes little sense. Relevant protections for data typically arise under the laws of the Member State where a person *resides*. In many cases, that will be a state other than the one where the service provider is established or has its legal representative (for example, the enforcing Member State). And the enforcing Member State often will have no way to evaluate whether the data at issue is subject to legal protections in the Member State where the target resides. Failure to give notice to affected Member States risks abrogating the fundamental rights of individuals whose data is targeted. It also means that providers might be compelled to disclose a person's data in situations where doing so would conflict with the law of the Member State where the person resides. Resolving those conflicts will be impossible, however, where the affected Member State is unaware that an order has been issued. The Regulation could address this concern by requiring the issuing authority to notify EPOs to the Member State where the person targeted by the order resides. This Member State will be in the best position to identify any applicable privileges and immunities that might apply to the data in question, and will have the strongest interest in defending these protections. This solution should not be unduly burdensome for authorities; in Microsoft's experience, only around 7 per cent of European law enforcement demands for user data involve targets located in a different Member State.

C. Requirement to Use EU Measures in Cross-Border Cases

Today, when Member State authorities in one Member State (for example, Belgium) seek disclosure of data from a provider located in a second Member State (for example, the Netherlands), they sometimes rely on domestic law and legal process (in our scenario, Belgian law) to do so. These domestic rules, however,

[22] ibid.

vary between Member States in terms of the types of protections and the levels of safeguards they provide. For example, some Member States might not require that a court review an order to disclose email content before that order can be served on the provider. Others might not require that the targets of such orders be given notice, or might not provide a clear path for service providers to challenge orders that violate fundamental rights. As a result, under current practice, a data subject located in one Member State may effectively be subject to the laws and legal procedures of a different Member State, which may provide fewer safeguards than the data subject's home country. Compliance with an order in one Member State may also require providers located in a different Member State to take steps that violate the laws of that second Member State, thus placing providers under the risk of conflicting legal obligations. This situation creates barriers to the free movement of services in the internal market. As the Commission noted in the Explanatory Memorandum to the proposal for an E-Evidence Directive:

> Harmonised rules at EU level are not only necessary to eliminate obstacles to the provision of services and to ensure a better functioning of the internal market but also to ensure a more coherent approach to criminal law in the Union. *A level playing field is also necessary for other fundamental premises for the good functioning of the internal market, such as the protection of fundamental rights of citizens* and the respect of sovereignty and public authority when it comes to the effective implementation and enforcement of national and European legislation.[23]

The e-evidence package provides an opportunity to address these issues and to ensure that the same rules apply across the Union in any case with a cross-border dimension. The best way to achieve these goals, however, is in the Directive rather than the Regulation. Since the Directive by its terms applies to *all* types of orders served on covered service providers, while the Regulation deals with only two discrete types of such orders (EPOs and EPrOs), implementing this fix in the Directive would ensure that it applies to all forms of criminal legal process and provides maximum protection for users. In particular, the Directive could provide that, where a service provider, in accordance with the Directive, has appointed a legal representative to receive and comply with orders for electronic evidence in criminal cases, authorities in Member States other than the home state of that representative must use an *EU-level* measure – and not a domestic one – to obtain such evidence. So in our example above, Belgian authorities would need to use an EU-level measure (such as an EPO) when demanding data from a provider established in the Netherlands, or whose legal representative is located there. Requiring authorities to use an EU measure, rather than a domestic one, means all users will enjoy the same protections across the EU, regardless of the Member State making the demand or where the provider is established or has its legal representative. This is appropriate from the perspective of the internal market, given the inherent

[23] Proposal for an E-Evidence Directive, 3 (emphasis added).

cross-border dimension of such cases – namely, that authorities in one Member State are serving orders on a representative located in a different Member State.

D. Empowering Service Providers to Challenge Overbroad or Otherwise Inappropriate Orders

In order for the E-Evidence Regulation to adequately protect fundamental rights, cloud providers must have a solid legal basis and clear procedures to challenge unlawful or otherwise inappropriate demands for user data. This is because, in many cases, the authority making the demand might not have access to the information needed to reveal that the order is overbroad or otherwise problematic. Consider the example of a criminal investigation involving four employees of 'Acme Company'. Investigating authorities might issue an order seeking all emails sent from the 'acmecompany.com' domain without realising that the company has thousands of employees who send emails from that domain – the vast majority of whom have no connection whatsoever to the crime under investigation. In the absence of an ability for service providers to challenge such an order, providers could be compelled to disclose the emails of *every* employee's email account – which could violate the right to respect for private life of many people who have nothing to do with the alleged crime. This could lead to the disclosure of irrelevant and confidential data in a manner wholly disproportionate to the scope of the investigation.

The proposed Regulation gives providers only very limited rights to challenge EPOs on overbreadth or similar grounds. Essentially, providers may challenge orders on such grounds only if, 'based on the sole information contained in the [EPO certificate] it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive'.[24] The Council general approach deletes even these narrow grounds for service providers to object to orders.[25] Empowering service providers to challenges overbroad orders is critical. In some cases, only service providers will have the ability to identify demands that overreach. By preventing cloud providers from challenging such orders, the proposed Regulation would also deprive providers of rights they might otherwise have under the law of the issuing and/or the enforcing state. By contrast, under the Council general approach, an EPO would be immune to any such challenge, leaving providers (and their users) with fewer protections for their rights than they might have under existing domestic law.

[24] Proposal for an E-Evidence Regulation, Art 9(5). The Regulation separately allows providers to object to an EPO if they do not hold the data in question or cannot comply for some other reason. See, for example, Art 9(3) (addressing situations where an EPO is 'incomplete, contains manifest errors or does not contain sufficient information to execute' the order); Art 9(4) (addressing situations where a provider cannot comply with an order 'because of force majeure or of de facto impossibility not attributable to' the provider).

[25] Council, Document 15292/18 (n 19).

E. A Mechanism to Resolve Conflicts with Third-Country Laws

Article 15 of the proposed Regulation sets forth an innovative procedure for service providers to object to EPOs where compliance would force the provider to take steps that conflict with third-country laws protecting privacy or other fundamental interests. It also sets out a process for courts in the issuing Member State to resolve such conflicts by sending the order to competent authorities in the third country for review. Although there are aspects of that procedure that should be refined, the overall approach is satisfactory, both because it helps protect the rights of users that might arise under foreign law and because it minimises the risk that providers will be placed into irreconcilable conflict-of-law situations.

Be that as it may, the Council general approach eliminates Article 15 and, in doing so, substantially weakens these safeguards.[26] First, the Council text no longer requires courts to communicate with third-country authorities to resolve identified conflicts of laws (it makes this optional). Since the Council text also prohibits service providers from disclosing that they have received an order, this means that third countries, including countries that work closely with the EU on important public-security and law-enforcement matters, might never know that EU authorities have forced the provider to violate their laws, making it impossible for them to object or to defend the underlying fundamental rights. Second, even where a court determines that enforcement of the order would violate third-country laws protecting fundamental rights, the Council text authorises the court to uphold the order. Third, the Council general approach gives providers only 10 days to file a reasoned objection setting out 'all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation'. In many cases, this will be insufficient time for providers to prepare such a complex analysis.

In order to address these concerns, Article 15 should be reinstated. To ensure that it fully meets the objective of avoiding conflicts of law, however, that proposal should also: (i) require courts, where they have identified a conflict with third-country laws protecting fundamental rights, to lift the order unless the competent authorities of the third country attest that there is no conflict; and (ii) provide opportunities to service providers to submit arguments and evidence directly to such courts as to the existence or nature of such a conflict. Ensuring that providers have the ability to alert judicial authorities when compliance with a Member State order would force them to violate third-country privacy or similar laws – and requiring authorities to work with third-country authorities to resolve those conflicts *before* forcing the provider to comply with an order – are essential for safeguarding that the fundamental rights of all users are fully respected, and that

[26] ibid.

service providers offering services both within and outside the European Union are not forced to violate one jurisdiction's laws solely in order to comply with the laws of a different jurisdiction.

V. Conclusion

As more information moves online and into the cloud, law-enforcement authorities will undoubtedly at times need to access that information, and online service providers will sometimes be best placed to provide it. But the rules and procedures governing such access matter to all of us. Ensuring that these rules fully respect fundamental rights and do not force providers to violate the laws of third countries are goals that everyone should support. The Commission's e-evidence initiative provides a unique opportunity for EU policymakers to achieve these goals in ways that are workable, preserve important European values and provide a model for the rest of the world.