**Challenges of obtaining electronic evidence from abroad**

**IAP summary of session:**

*This workshop will address challenges in the cross-border access to electronic evidence in the context of state-to-state as well as in public private cooperation. In recent decades, important international instruments have been introduced or initiated to assist with cross border access to electronic evidence. However, there are still largely divergent laws and procedural standards across jurisdictions that challenge practitioners in successful trans-border cooperation or direct access to electronic evidence.*

*Multinational online service providers hold an important key for the trans-border access to electronic evidence. While there are examples of good practice, not all of them are ready or willing to cooperate with foreign criminal justice authorities.*

*Prosecutors and other criminal justice actors will examine how the existing tools of cross-border access to electronic evidence work in practice. The workshop will explore how the newly designed and emerging international instruments will change the environment. The role of multinational service providers will also be discussed alongside examples of successful and flawed cooperation with them.*

**Synopsis of presentation:**

The presentation will briefly consider some of the common challenges in obtaining electronic evidence – both in relation to the nature of the material itself and in relation to the MLA process more broadly. Two initiatives that may assist law enforcement and prosecutors in obtaining electronic material will then be discussed – bilateral data access agreements and powers of compulsion to access passwords to electronic devices.

**Presentation:**

Rapid technological advancements and the digitisation of society has had a significant impact on the investigation and prosecution of offences. Fifteen years ago, evidential packages in both simple and complex cases would have consisted of statements from eye-witnesses, statements from law enforcement and documentary material. Now, electronic devices that we have in our homes and carry around with us daily hold a wealth of information, with an ever-increasing number of cases involving electronic material – either as evidence or unused material. A European Commission Memorandum in 2019 noted that more than half of all criminal investigations now require access to cross-border electronic evidence. Also, where electronic evidence does exist in a case, the scale of it can be enormous. In one of our recent cases, we were faced with approximately 32 million files across all devices. We identified which file types (excluding emails) that could contain relevant material and were left with more than 1.3 million. In addition there were more than 617,000 relevant email files.

Chat backups identified on computers initially totalled almost 500,000 messages – many of which were in foreign languages. The review process filtered these to 24,000 relevant unused messages and 10,000 were used in evidence. It’s apparent that electronic data can both be exploited by criminals but can also be integral in building a case against them for prosecution.

There are a range of factors that come into play when seeking to access electronic evidence for use in criminal investigations and prosecutions – legal considerations, logistical constraints, national security considerations, data protection rights, commercial interests, and civil liberties. As the need for cross-border access to electronic evidence grows, the international community must become more agile and responsive to ensure that opportunities to preserve and gather such evidence are not lost, whilst ensuring that we still respect the appropriate data protection rights.

The formal mutual legal assistance (MLA) system remains a critical tool in the evidence-gathering process, and one which provides an important legal framework for the seeking and provision of assistance for use in the investigation and prosecution of criminal offences.

However, the mutual legal assistance system faces significant challenges in its operation, requiring the international community to consider alternative options to ensure the efficient and effective access to electronic evidence needed to successfully prosecute serious and organised crime, whilst also having due regard for sovereignty and privacy.

Those challenges are well documented and include:

– differences in legal and procedural frameworks, which can range from different approaches to the legal basis for providing MLA or different grounds on which MLA can or must be refused

- different legal and procedural requirements for obtaining certain types of assistance such as content data

- language barriers

- a delay or an inadequate or no response at all, which can sometimes be attributable to a lack of resources in the requested State

- a lack of cooperation between the executing agencies in the requested State

- the nature or quantity of the evidence sought

- the complexity of the legal processes that have to be followed before the request can be carried out

- resource constraints in the requesting State that impact the review and preparation of material received for court use and/or disclosure

- a combination of the above.

One significant challenge in obtaining electronic evidence is linked to retention periods. Many service providers will only retain data for a limited period – 30 days, for example – unless a preservation order is put in place before the data is destroyed. Whilst the process to seek a preservation order is relatively straightforward, it presupposes that law enforcement are aware of the existence of, and potential significance of, electronic material within that same timeframe. In large-scale, complex investigations or cases of historic offending – often in relation to sexual offences – the fact that relevant electronic material may exist is not known for months or even years after the offence took place. By that time, any opportunity to preserve the data has been lost. Whilst that’s not to suggest that all electronic data should be kept indefinitely, the risk of a very short limitation period is that key evidence and material is lost before its potential significance – or even its existence – is known. Additionally, preservation orders require regular renewal which is resource-intensive and, particularly in long-running investigations, runs the risk of deadlines for renewal being missed and data being deleted.

Differences in legal systems and standards are also problematic. Probable cause, the legal standard that must be met to access content data in the US, has no direct comparable equivalent in the UK, for example. Whilst close collaboration between prosecutors and the provision of training assists, it can still be difficult for prosecutors to properly understand and articulate the basis for seeking data when operating within a legal system that is different to their own.

Authentication of electronic evidence is another area where some service providers could look to adopt best practice to assist law enforcement. In some jurisdictions, the electronic data itself is potentially inadmissible if it is not accompanied by a continuity statement or a statement of authenticity. Whilst such data can still be considered for disclosure purposes, it is vital that evidential use can still be made of relevant material.

It is apparent that, whilst the MLA process can be used to obtain electronic data, it is not without its challenges. Delay is also a relevant factor – as we all know, the MLA process can be resource-intensive and slow which, particularly at the investigative stage, can have a real impact on investigations. Consequently, new and innovative ways of obtaining electronic data, whilst still operating within the appropriate legal frameworks, have to be considered.

I would like to briefly mention two initiatives. The first does not expressly relate to obtaining electronic data across borders, but rather to enhanced police powers to obtain electronic data by accessing the device on which it is stored. In certain circumstances, UK police can serve a notice on a suspect requiring the disclosure of a PIN or password for an electronic device that has been lawfully seized. Once the notice has been served, it is a criminal office to refuse to provide the information that is sought, punishable by up to five years’ imprisonment in a national security or child indecency case, and by up to two years’ imprisonment in all other cases.

The second initiative is the Data Access Agreement which was signed by the US and the UK in 2019 and which will come into force in October 2022. It will allow investigators from each of the two countries to gain better access to vital data to combat serious crime in a way that is consistent with our shared values and mission of protecting our citizens and safeguarding our national security.

The Data Access Agreement will allow information and evidence that is held by service providers in either the US or the UK, and which relates to the prevention, detection, investigation or prosecution of serious crime to be accessed more quickly than ever before, and without utilising the traditional MLA route. It allows for an order obtained in one jurisdiction to be served directly on a service provider in the other jurisdiction to require that service provider to produce electronic evidence when necessary for the investigation or prosecution of a serious crime.

Legislative change was required in both the UK and the US to remove legal barriers that would otherwise prevent compliance with court orders issued by another country. In the UK, the legislation was designed to overcome the lack of extraterritorial scope and to enable certain officers to apply for an order relating to data held outside of their jurisdiction. The agreement maintains strong oversight and protections, upholding democratic and civil liberties standards whilst also improving our collective ability to tackle serious crime.

This is an innovative and progressive agreement, which is the first of its kind. It will create a much more streamlined way in which to obtain electronic data, and significantly reduce the time that it takes to obtain such data. It has the potential to transform the way in which we prevent, investigate, detect and prosecute serious crime. The Act represents a significant move away from the long-standing conventional approach to obtaining communications data stored overseas but has the potential to enable law enforcement agencies to obtain electronic data in days, rather than weeks – the importance of which cannot be underestimated, given the fast-moving pace of investigations and the need to ensure that evidence is available for trial.

To conclude, obtaining electronic data quickly and efficiently to assist in the prevention and detection of serious crime is essential. Technological advances and the growth of digital material means that law enforcement and prosecutors need to look at novel ways to obtain such data, rather than simply continuing to rely on the slower MLA process. Collaboration and cooperation between countries is key – working together to identify solutions which improve our collective ability to tackle serious crime and to protect our citizens.