Independent Commission on UK - EU Relations

POLICE ACCESS TO ELECTRONIC EVIDENCE:

UK-US AGREEMENT FINALLY COMES INTO FORCE

Gemma Davies

ABOUT

INDEPENDENT COMMISSION ON UK-EU RELATIONS

The Independent Commission on UK-EU Relations is a timebound commission which examines the impact of the Trade and Cooperation Agreement (TCA) and Northern Ireland Protocol (NIP) on the UK.

As well as looking at impacts on different sectors of the economy we look more broadly at impacts on sectors including security and defence, health, education and human rights.

There are 13 members of the Commission from business, journalism, civil society and academia, along with a team of advisors. The intended outcome of the Commission is to recommend changes to the TCA and Protocol which, if implemented, would improve outcomes for UK sectors and the people who live and work in the UK.

There recommendations will be developed in collaboration with UK and EU politicians and relevant officials. We confer with parliamentarians from all parties as well as with regional and devolved and local politicians and party staff.

As well as informing parliamentarians and political parties the Independent Commission will inform the public of its work, both to highlight and explain challenges created by current arrangements and potential amendments.

For further information see **www.ukeucommission.org**

COMMISSION CO-CHAIRS

Mike Clancy: Co-Chair, Independent Commission on UK-EU Relations

Janice Hughes CBE: Co-Chair, Independent Commission on UK-EU Relations

CONTACTS

Mike Buckley: Director, Independent Commission on UK-EU Relations – mike@ukeucommission.org

AUTHOR

Gemma Davies: Associate Professor, Durham University – gemma.davies@durham.ac.uk

CONTENTS

Exponential increase in electronic evidence which may be relevant for the purposes of criminal investigation or prosecution resulting in an **84%** increase in requests for evidence to the main service providers between 2012 and 2018.

It has been three years since the UK and the US signed an international agreement on access to electronic evidence.

However, it only came into force on October 3, 2022. The joint statement released on July 21, 2022, confirms that the aim of the Agreement is to "allow information and evidence that is held by service providers within each of our nations and relates to the prevention, detection, investigation or prosecution of serious crime to be accessed more quickly than ever before." Historically such evidence has only been obtainable through mutual legal assistance treaties (MLATs). Such treaties are subject to judicial scrutiny in both the state requesting the evidence and, in the state, providing the evidence. However, MLATs were said to be too slow and bureaucratically cumbersome, often taking over a year to be actioned. The Covid 19 pandemic only exacerbated delays. This is in part due to the exponential increase in electronic evidence which may be relevant for the purposes of criminal investigation or prosecution resulting in an 84% increase in requests for evidence to the main service providers between 2012 and 2018.

The US responded to these difficulties by passing the CLOUD Act in 2018 which explicitly provided for warrants issued by a US judge to be enforceable against US internet service providers regardless of whether the data the warrant sought was held in the US or not. A second part of the Act permitted the US government to enter into executive agreements granting foreign access to data stored by US service providers. Under US law service providers were prohibited from disclosing the content of electronic communications directly to foreign governments. Without a CLOUD Act agreement law enforcement in the UK would have to obtain a warrant for disclosure through a MLAT.

The UK responded by passing the Crime (Overseas Production Orders) Act 2019 (COPOA). This provides a mechanism for a UK judge to issues an order requiring the production of stored electronic information located or controlled outside of the UK if an international agreement has been signed with the government of the state where the data is requested. The UK was the first state the US signed such an agreement with. If it had still been a member of the European Union competence to enter such an agreement would have fallen with the EU. In September 2019 the EU announced the start of formal negotiations with the US on an EU-US agreement on electronic evidence but little progress has been made. The fact that the UK was able to negotiate so quickly with the US was an example of its flexibility post Brexit to chart closer relations with key partners.

WHAT IS THE AGREEMENT?

It enables UK law enforcement and prosecution agencies to send a request for data directly to the service provider who holds the data if they operate in the US – and vice versa. The Investigatory Powers Commissioner monitors compliance by UK authorities with the terms of the agreement. Each party complies with their own domestic legislation when making a request for data. The order is only available under the agreement for the purpose of the prevention, detection, investigation, or prosecution of serious crime. This is defined as a crime punishable with a maximum term of at least three years.

The order can cover content data (such as messages and pictures), traffic data and subscriber information. The UK cannot request access to data on a US person or person located in the US, but the reciprocal provision is not identical. US law enforcement agencies can request data from UK citizens but not anyone who is in the UK (whether they are a UK citizen or not). There is no requirement of the service provider to remove encryption and non-compliance with the order is governed by the legislation of the country making the request.

WHY DID IT TAKE SO LONG FOR THE AGREEMENT TO COME INTO FORCE?

There is no official explanation for why the agreement has taken four years to come into force. However, although the UK has a data adequacy agreement with the EU, it was granted with warnings. Actual and potential data-transfer relations between the US and the UK were cited as an area of concern by the European Data Protection Board. The EDPB highlighted that the CLOUD Act agreement *'may affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act agreement.'* The final text of the UK adequacy decision states that *'special attention will be paid to the application in practice of the United Kingdom's rules on transfers of personal data to third countries'.*

DOES THE UK-US AGREEMENT ADEQUATELY PROTECT EU CITIZENS?

The UK-US Agreement specifically allows third country person (TCP) targeting. TCPs are those neither located in the UK or the US but in a third country.

For example, the US requests access to emails held in a server in the UK which were sent by a French citizen living in Germany. In this scenario the only forum potentially open to challenge such an order for production of data relating to TCP (if it is even known about) would be in a US court. US courts do not extend Forth Amendment protection to those outside of the US. Under Article 5(10) of the Agreement there is a requirement on the requesting state to notify the appropriate authorities in the third country where the person is located (in the scenario above, Germany) but the target (the French citizen) does not need to be notified. Notification can be delayed until after the data has been obtained if there are national security concerns or it would impede the conduct of an investigations.

This is a broad exception and would likely arise in many, if not all, cases. Even if the state was notified there is no clear mechanism for it to provide its objection. Another safeguard set out in Article 5(11) is that the service provider may 'raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order.' Such concerns can ultimately be heard by the issuing State's Designated Authority. This places a high degree of trust in the service provider who, once the order is issued, is the only body capable of protecting TCP rights. Their ability to carry out this role may depend on their capacity considering the short timeframe they have to respond and number of requests they may be dealing with. Service providers may also not have enough information about the target or knowledge of the laws of other countries to identify relevant 'specific' objections. Considering the US's data dominance, the EU is likely to still be concerned about the level of protection the UK-US Agreement offers to EU citizens.

CONCLUSION

It is unclear what impact, if any, the Agreement will have on the UK's data adequacy decision. It may be that we will have to wait for a challenge in the CJEU. The EU court has a history of strong intervention in the field. For example, it struck down EU-US Privacy Shield. Although the CJEU has no jurisdiction over the US-UK Agreement it does over the UK-EU data adequacy decision. The primary concern in the Schrems II judgment was the lack of proportionality in US intelligence surveillance and a lack of redress for individuals' complaint. Whilst there is no substantive change in UK data protection law the Commission has already shared its concerns about the protection of EU citizens in the Agreement and will be watching its application in practice closely. If signing the Agreement with the US is an example of a 'Brexit bonus' then what happens next will be of intense political interest.

POLICE ACCESS TO ELECTRONIC EVIDENCE:

UK-US AGREEMENT FINALLY COMES INTO FORCE

UKEUCommission
uk-eu-commission
@UKEUCommission

ukeucommission.org

The Commission is run by UK EU Future Ltd, based at Aizlewoods Mill, Nursery Street, Sheffield S3 8GG

Company number **13742325**