**Royal United Services Institute**
for Defence and Security Studies

BRIEFING PAPER

# No Deal, No Data?

## The Future of UK–EU Law Enforcement Information Sharing

Alexander Babuta

**ACKNOWLEDGEMENTS**

The author is very grateful to Sir Rob Wainwright, Andrew Glazzard and Malcolm Chalmers for providing helpful feedback on an earlier version of this article. Thanks are also due to the RUSI Publications team for their editorial input, in particular Melanie Bell and Emma De Angelis.

## SUMMARY

- The UK has been deeply embedded in EU security mechanisms for many years. In fact, the UK was instrumental in developing many of the capabilities which are now relied upon to facilitate cooperation and data sharing between member states' law enforcement agencies (LEAs). However, with the UK set to leave the EU in a matter of weeks, there remains considerable uncertainty concerning the UK's future position in the EU's security architecture.
- If the UK exits without a deal, access to EU databases will end, leaving UK LEAs with a major capability gap, and potentially causing significant damage to UK and European security.
- If a deal is reached before the UK leaves, a new security arrangement would need to be agreed before the end of the transition period for the UK to retain access to EU tools.

The UK government must now decide on the minimum level of access to EU databases it is prepared to accept post-Brexit. The EU negotiators must likewise decide whether they are prepared to create precedents for third country access to EU tools, as part of a new bespoke security arrangement.

There are three possible scenarios for UK–EU law enforcement information sharing post-Brexit, which would each provide the UK with different levels of access to EU tools and capabilities:

- **Option 1:** In a no-deal scenario, the UK would lose access to all information systems and databases established on the basis of EU law, leaving UK LEAs with a major capability gap. The UK could then seek to negotiate new agreements with the EU to regain limited access to certain tools as a third country.
- **Option 2:** If a deal is reached before the UK leaves, the UK would retain access to all EU systems for the duration of the transition period. During this time, the UK may be able to negotiate new agreements to maintain limited access to certain tools as a third country following the end of the transition period.
- **Option 3:** The UK government's desire is to establish a new bespoke Internal Security Treaty, which would provide the UK with permanent access to most (if not all) EU information systems following the end of the transition period.

In relation to Option 1, cutting the UK off from all EU information systems would undoubtedly weaken UK and European law-enforcement capabilities, as these tools are relied upon to ensure efficient data sharing between member states' LEAs. Furthermore, the UK is one of the largest contributors of intelligence to EU databases,[1] so such a move may damage member states' security as much as it damages UK security.

Option 2, in which the UK retains limited access to certain tools as a non-Schengen third country, would place the UK in a similar category to countries such as the US, Canada and Australia, but with much more limited access than Schengen Area associated states (Norway and Switzerland). This would represent a major loss of capability, albeit not to the same extent as a no-deal outcome.

The UK government's proposal to retain access to all EU tools is ambitious, and the EU has given no indication that it will be willing to grant such unprecedented access to a third country. These proposals may also prove problematic from a legal perspective. The processes, databases and systems to which the UK wishes to maintain access are established on the basis of EU law, passed through the Court of Justice of the European Union (CJEU). The EU would therefore need to develop new legal mechanisms to ensure that the UK continues to abide by legislation governing the use of these tools and associated data-protection provisions.

## OPTION 1: NO DEAL, NO ACCESS TO EU TOOLS

If the government fails to negotiate a new deal that is passed through Parliament before 29 March (assuming Article 50 is not extended through an amendment of the EU (Withdrawal) Act or revoked through enactment of primary legislation), the UK will leave the EU without a deal and will immediately move to third-country status, with no transition period. The UK would lose access to all information systems and databases established on the basis of EU law, of which there are more than 40. The UK's access to EU capabilities would therefore fall below that of other third countries such as the US, Canada and Australia. Loss of access to these systems would significantly weaken UK LEAs' intelligence coverage, with the following tools being of particular concern in this regard:

- The Schengen Information System (SIS) II allows LEAs in participating states to share real-time information on persons of interest, objects and vehicles, including European Arrest Warrants (EAWs).[2] In 2017, the UK created over 1.4 million alerts on SIS II and registered almost

1. HM Government, *The Future Relationship Between the United Kingdom and the European Union* (London: The Stationery Office, 2018), p. 62.
2. European Commission Migration and Home Affairs, 'Schengen Information System', last updated 14 February 2019, <https://ec.europa.eu/home-affairs/

10,000 hits against alerts put on the system by other countries.[3] Losing access to SIS II would deprive UK LEAs of the capability for real-time reciprocal exchange of information with member states. For example, an individual who was wanted in another member state could pass through the UK border undetected, because their EAW would no longer sync with UK systems.

- The Europol Information System (EIS) is Europol's central criminal information and intelligence database, containing information on more than 86,000 suspected criminals and terrorists.[4] EIS allows member states to check whether information on people or objects of interest is available beyond national jurisdictions. Losing access to EIS would mean that UK investigators would no longer have access to a centralised portal to check whether information on a subject of interest existed in any other member states' systems. UK LEAs would need to make separate requests to each member state to check whether they held relevant information.
- The Europol Secure Information Exchange Network Application (SIENA) is a secure platform allowing member state LEAs to swiftly exchange sensitive and restricted data.[5] Several third countries also have cooperation agreements with Europol, granting them access to SIENA. SIENA connects UK LEAs with 1,200 agencies in 47 countries and enables EU asset-recovery offices (AROs) to exchange information about assets to be seized, frozen or confiscated. If UK LEAs lost access to SIENA, they would become dependent on bilateral information-sharing mechanisms, which may cause lengthy delays in the retrieval of time-sensitive intelligence.
- The European Criminal Records Information System (ECRIS) enables rapid exchange of information on criminal records and convictions across EU member states.[6] Between 2014 and 2016 the UK was among the top three most active member states on ECRIS.[7] If the UK lost access to ECRIS, requests to EU member states for information on criminal records and convictions would no longer be automated, and

The UK would lose access to all information systems and databases established on the basis of EU law

what-we-do/policies/borders-and-visas/schengen-information-system_en>, accessed 18 February 2019.

3. HM Government, *The Future Relationship Between the United Kingdom and the European Union,* p. 57.
4. Europol, 'Europol Information System (EIS)', <https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system>, accessed 18 February 2019.
5. Europol, 'Secure Information Exchange Network Application (SIENA)', <https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena>, accessed 18 February 2019.
6. European Commission, 'European Criminal Records Information System (ECRIS)', <https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en>, accessed 18 February 2019.
7. HM Government, *The Future Relationship Between the United Kingdom and the European Union,* p. 58.

data would not be provided in a standardised format. There would no longer be timelines for responses to requests, meaning UK LEAs may remain unaware of a detained individual's criminal history.

- Passenger Name Record (PNR) capabilities allow for reciprocal exchange of passenger data between member states, enabling Passenger Information Units (PIUs) to work together to jointly identify travel patterns.[8] The UK was at the forefront of EU-level PNR capability development and was the first EU country to have a functioning PIU. In the event of no deal, the UK would lose access to the same PNR capabilities it was instrumental in developing. It would become slower and more difficult for the UK and member states to share information about suspicious travel, resulting in fewer opportunities to identify and intercept suspects.
- Additionally, the UK would not be able to participate in Prüm, a new EU data-exchange tool that enables member states to share DNA, fingerprint and vehicle data in real time.[9] While Prüm capabilities are yet to be implemented operationally, the government's White Paper states that the UK is now ready to begin exchanging DNA and fingerprint data using Prüm, and that the vast quantity of DNA and fingerprint data held on UK police databases would allow the UK to make 'a substantial contribution to this system'.[10]

In the absence of EU data-sharing capabilities, UK LEAs would become reliant on the bilateral police attaché network, run principally by the National Crime Agency (NCA), and INTERPOL information systems, which are far less integrated than EU systems. The result would be a marked reduction in monitoring coverage of offenders and suspects across Europe. Considering all of the evidence, it is difficult to see a scenario in which a no-deal outcome does not cause significant damage to UK and European security.

## OPTION 2: NEGOTIATING LIMITED ACCESS TO TOOLS AS A THIRD COUNTRY

Following its departure from the EU, the UK could seek to negotiate bespoke agreements to allow continued, limited access to certain tools and measures, albeit with several caveats. If a deal is in place by the time the UK leaves, such an agreement could be negotiated during the transition period, during which the UK would retain full access to EU systems. In the event of a no-deal

8. European Commission Migration and Home Affairs, 'Passenger Name Record (PNR)', <https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en>, accessed 18 February 2019.
9. UK Parliament, 'Select Committee on European Union Eighteenth Report, Chapter 2: Background', 2017, <https://publications.parliament.uk/pa/ld200607/ldselect/ldeucom/90/9005.htm>, accessed 18 February 2019.
10. HM Government, *The Future Relationship Between the United Kingdom and the European Union,* p. 59.

departure, the UK would seek to regain access to EU systems following a period in which access is cut off altogether.

There are existing precedents for third-country access to some EU tools, such as SIS II, Prüm, EIS and PNR, but no precedent for others, most notably ECRIS. The level of access granted varies by tool and by country, with only Schengen Area associated states (Norway and Switzerland) being granted full access to any EU data system.[11]

Norway and Switzerland have full access to SIS II and Prüm, but do not have voting rights in EU-level working groups or experts' committees. Non-Schengen-associated third countries – such as the US, Canada and Australia – have no access to the systems. If the UK were to seek the same status as Schengen Area associated states, this would require the EU to create a precedent for a non-Schengen-associated third country to be granted access. There is no guarantee that the EU negotiators would be prepared to create this precedent, and if they were, the process would be legally complex and would take time.

Several non-Schengen-associated third countries, such as the US and Canada, have operational agreements with Europol which provide indirect access to EIS, but data must be uploaded or queried via a pool of Europol operatives. In the case of PNR, only the US, Canada and Australia have agreements that provide for transmission of PNR by air carriers to authorities in third countries, but these agreements do not provide for reciprocal exchange of PNR data, and do not enable third countries to work with member states' PIUs to jointly identify travel patterns.

If a new agreement is not in place by the end of the transition period, the Withdrawal Agreement states that the UK would have continued access to some systems for a limited period.[12] The UK would be entitled to use SIS II for no longer than three months after the end of the transition period, to the extent strictly necessary for the purpose of exchanging supplementary information where there was a hit before the end of the transition period. The UK would also be entitled to use SIENA for no longer than one year after the end of the transition period.[13]

In the case of both SIS II and SIENA, the UK will be required to 'reimburse the Union for the actual costs incurred by the Union as a consequence of facilitating the United Kingdom's use of' the systems.[14] If, by the end of the

11. HM Government, 'Technical Note: Security, Law Enforcement and Criminal Justice', 24 May 2018.
12. European Commission, 'Draft Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as Agreed at Negotiators' Level on 14 November 2018', 2018, p. 6.
13. *Ibid.,* p. 113–14.
14. *Ibid.,* p. 84.

transition period, an agreement has been reached that provides the UK continued access to these tools (granting it the same status as Schengen Area associated states), as a third country it would inevitably be required to make a financial contribution to the EU to cover the costs of using these systems. The EU's cost estimates have been communicated to the government but are not public, so it is not possible to speculate on what continued access might cost.

The Agreement also states that the UK would lose access to ECRIS and PNR capabilities.[15] The EU's expectation may be that an agreement will be reached during the transition period which will provide the UK with limited, indirect access to ECRIS, and the same limited access to PNR as the US and Australia. From a security perspective, it is in the EU's interest to continue sharing criminal records and conviction data with the UK, and to allow the UK to continue working with member states' PIUs to jointly identify travel patterns. However, there is no legal basis for a third country to have access to ECRIS or PNR capabilities, and even if the EU were to create such a precedent, it is likely to come at a cost. The UK would be paying to use the very same systems that it was instrumental in developing.

The UK would be paying to use the very same systems that it was instrumental in developing

## OPTION 3: A BESPOKE INTERNAL SECURITY TREATY, FULL ACCESS TO EU TOOLS

The UK government's desired outcome, as proposed in the White Paper, is to negotiate a bespoke Internal Security Treaty during the transition period, which would provide the UK continued access to most (if not all) EU tools and instruments.

The government's assessment is that 'a piecemeal approach to future cooperation, drawing on precedents for EU agreements with third countries on individual measures … or functions … would result in a limited patchwork of cooperation falling well short of current capabilities'.[16] Instead, the government is requesting a strategic cooperation agreement that would provide a legal basis for sustaining existing cooperation on the basis of existing EU measures.

In the case of SIS II and Prüm, the UK is requesting the same status granted to Schengen-associated third countries. However, in the case of PNR, ECRIS, EIS and numerous other tools, the government is requesting the EU to create a precedent for a third country to be granted full access to capabilities that are currently reserved for fully paid-up members of the Union.

It is clear why a new Internal Security Treaty is the UK government's preferred outcome: anything less would reduce UK LEAs' capabilities and cause unnecessary damage to what is a highly effective security partnership.

15. *Ibid.,* p. 15.
16. HM Government, 'Technical Note: Security, Law Enforcement and Criminal Justice', p. 1.

The government maintains that the Treaty could be enshrined in EU law, being negotiated 'according to an Article 218 TFEU [Treaty on the Functioning of the European Union] procedural legal base with citation of substantive legal bases … in relevant Council Decisions'.[17] However, as stipulated in the political declaration for the future relationship between the EU and the UK, any future arrangements 'should reflect the commitments the UK is willing to make that respect the integrity of the Union's legal order, such as with regard to alignment of rules and the mechanisms for disputes and enforcement including the role of the Court of Justice of the European Union (CJEU) in the interpretation of Union law'.[18] Negotiating such a security treaty would therefore require establishing a dispute resolution and enforcement function for the CJEU, or for another equivalent body with the necessary legal authority.

Moreover, negotiating such a complex legal agreement would take time, and a successful agreement is by no means guaranteed. However, despite these legal and political difficulties, this may turn out to be the only viable option for both sides to maintain current levels of UK and European security. The UK makes a disproportionate contribution to EU data systems and cooperation arrangements, and it is in neither party's interest to unnecessarily impede this flow of critical information.

## CONCLUSIONS

- Cutting the UK off from EU databases would unnecessarily weaken UK LEAs' capabilities, and could cause significant damage to both UK and European security.
- Replicating existing precedents for third-country access to EU tools would not ensure efficient exchange of time-sensitive information and may prove impracticable given the high volume of current real-time data sharing.
- The only way to ensure that current levels of security are maintained is for both parties to negotiate a bespoke permanent security arrangement. The EU must consider creating new precedents for a third country to be granted access to certain critical databases, given the disproportionate contribution the UK makes to EU information systems.

17. *Ibid.,* p. 6.
18. European Commission, 'Draft Political Declaration Setting Out the Framework for the Future Relationship Between the European Union and the United Kingdom', p. 15.

# ABOUT THE AUTHOR

**Alexander Babuta** is a Research Fellow in National Security Studies at RUSI. His research focuses on policing, intelligence and technology, particularly the use of big data, artificial intelligence and machine learning. He holds an MSc with Distinction in Crime Science from University College London.

**About RUSI**

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.



Published in 2019 by the Royal United Services Institute for Defence and Security Studies.




**Royal United Services Institute**
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)