DATA PROTECTION, INTELLIGENCE-SHARING AND BREXIT: THE PATH AHEAD?

School of Law, The University of Manchester

1. Introduction

As technology advances and the world moves towards an unprecedented use of the internet, the importance of cyber security becomes ever more imperative. This applies not simply for individual users frequently accessing the internet for recreational or professional purposes, but on a grander scale, for the state that must contend with ever-growing threats to national security from cyber criminals. Whilst there are on-going developments to enhancing the UK's cyber security capacity, the current uncertainty around the ramifications of Brexit have meant that the UK's cyber security strength has been called into question. In particular, what impact, if any, will Brexit have on the UK's cyber security position?

This article deals with two distinct issues within the overarching area of cyber security. The first part of the article will deal with data protection and how the UK will respond to EU data protection laws. In short, this is quite a quick area to address, given the decisions that have already been made on EU laws such as the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NISD). The second part of the article, however, will highlight the real difficulties surrounding Brexit and focus on intelligence sharing. This is an area that is on tremendously shaky ground as far as strong intelligence cooperation is concerned between the UK and the EU. Information sharing will undoubtedly be affected by Brexit and this article will attempt to consider the impact and possible options for the UK.

2. Data Protection

One of the main issues concerning cyber security and Brexit has been the implementation of the General Data Protection Regulation (GDPR)[1] and whether the safeguards that are at the forefront of the GDPR will be translated into the British domain once Brexit takes place. The simple route, that of the UK going ahead with its adoption even after Brexit, has been confirmed. In its 'Cyber Security and Regulation and Incentives Review'[2], the Government stated that it will apply the GDPR from May 2018; indeed, it has also viewed the GDPR as merely a legislative crystallisation of many best practices that the Information Commissioner's Office (ICO) already applies. Additional incentives from the GDPR will include mandatory violation reporting to the ICO and customers; provision of data protection impact assessments; and stricter penalties. Therefore, it seems that in terms of EU data protection laws, the threshold will match the EU. UK strength in this area was reinforced by the Queen's speech in June 2017, which declared that '[a] new law will ensure that the United Kingdom retains its

[1] EU General Data Protection Regulation, available at http://www.eugdpr.org/; Information Commissioner's Office, 'Overview of the General Data Protection Regulation (GDPR), available at < https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>.

[2] HM Government, 'Cyber Security Regulation and Incentives Review', December 2018, available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf>.

world-class regime protecting personal data, and proposals for a new digital charter (…) brought forward to ensure that the United Kingdom is the safest place to be online.'[3]

The UK adopting the GDPR certainly alleviates complexities and lacuna that would have arisen had the directive been rejected by the UK. It ensures that high data protections will continue, if not, propelled. Whilst data protection has always been the UK's strong suit, with UK laws including the Communications Act 2003[4], the Privacy and Electronic Communications (EC Directive (Regulation) 2003[5], the Data Protection Act 1998[6] and the Computer Misuse Act 1990[7], there are other important EU directives that the UK will need to consider.

Following the European Council's adoption of the Network and Information Security Directive (NISD) in May 2016, there were new European rules dealing with issues such as cooperation between member states, standardisation of cyber security capabilities, enhanced security measures within different industries and the implementation of an EU strategy on cyber threats. The NISD consolidated and enhanced previous directives 2002/58/EC and 2002/21/EC requiring member states to put in place a national network and information security scheme and guarantees that personal data and relevant structures are protected. The NISD places emphasis on cooperative relationships between public and privates bodies. This is to ensure that states can effectively and rapidly provide warnings on unwanted occurrences and risks for an organised approach. Under the NISD, operators of crucial service providers will be under an obligation to adhere to strict risk management and reporting requirements. This is clearly vital given that the Department for Culture, Media and Sport have themselves affirmed that cyber risk is one of the biggest threats to UK businesses.[8] Again, this may not be too much of an issue, since the UK has also confirmed that the NISD will be implemented in 2018. Nonetheless, it is worth pointing out that whilst implementation of the GDPR and NISD may indicate a bit more certainty as far as data protection law is concerned, the politically charged nature of Brexit has undoubtedly shrouded cyber intelligence cooperation under a cloud of ambiguity. It is this area that will be most affected by Brexit and will be discussed in the next section.

3. Intelligence Sharing and Cooperation

Outside of the EU, the UK still has very strong capabilities that equal the EU in many respects and therefore has the ability to tackle potential cyber risks. The European Union Agency for Network and Information Security (ENISA) is deemed the centre for expertise on cyber security in Europe. It works closely with member states and the private sector to deliver advice, solutions and general cyber security assistance. It also functions as a platform for information and cyber security vulnerability sharing. The UK has now established the equivalent body in the form of the National Cyber Security Centre.

Whilst many commentators have tended to view the UK's exit from the Europe Union as detrimental for cyber security, the establishment of a National Cyber Security Centre in 2016 in many ways could dispute that opinion. The National Cyber Security Centre (NCSC) is the first UK consolidated centre on cyber security, which merges parts of GCHQ (for example, the older CESG), the Centre for Cyber

[3] Gov.uk, 'Queen's Speech 2017', 21 June 2017, available at https://www.gov.uk/government/speeches/queens-speech-2017.
[4] Communications Act 2003, c. 21, Part 1.
[5] The Privacy and Electronic Communications (EC Directive) Regulation 2003, No. 2426.
[6] Data Protection Act 1998, c. 29.
[7] Computer Misuse Act 1990, c.18.
[8] Department for Culture, Media & Sport and National Cyber Security Centre, gov.uk, 'Almost half of UK firms hit by cyber breach or attack in the past year', 19 April 2017.

Assessment, Computer Emergency Response Team UK and the cyber part of the Centre for the Protection of National Infrastructure. It brings together unique expertise and works closely with governmental agencies, law enforcement bodies and British, as well as international, intelligence agencies. Whilst it has only recently been established, its creation and general role must not be overlooked and already surpasses the cyber security protection capacity of many other European and non-European member states.

As part of its strategy, the NCSC included an Active Cyber Defence programme, which includes fixing the underlying infrastructure protocols; instilling confidence in the authenticity of emails through the tackling of phishing attacks; 'looking for badness' and taking it down; filtering DNS to manage impact; driving the UK software ecosystem to be better; providing public sector organisations a web check service and generally working with government closely to enhance cyber security; encouraging innovative alternatives for identity and authentication; providing owners and operators of critical national infrastructure with more help; and more generally, finding effective ways of responding to adversaries that will evolve over time. The work of the NCSC will continuously produce data and evidence better comprehend cyber-attacks and the efficiency of their defence approaches.[9]

The UK is also part of the Cyber Security Information Sharing Partnership (CiSP), a subset of CERT-UK. At the EU level, the enforcement of cyber security laws and policy is undertaken by the National Data Protection Authorities. In the UK, this is a role undertaken by Ofcom and ICO. Responsibility for the prevention and response to serious cyber attacks in the EU is held by the Computer Security Incident Response Team (CSIRTs) and the European Cybercrime Centre. Again, the UK matches these capabilities via the National Cyber Crime Unit of the National Crime Agency (NCA), together with GCHQ and the cyber units in each one of the nine Regional Organised Crime Units. Finally, cyber security information sharing across the EU is performed by the EU's NISD Cooperation Group; being part of the group is conditional upon the implementation of the NISD.[10]

For the UK, this latter point would have posed problems had it not decided to move forward with the NISD. Given that the UK will be implementing the NISD[11], it should be able to benefit from the NISD Cooperation Group. The NISD should be welcomed, given that it offers a sound and practical strategy to combat cyber risks and allow for strategic planning, coordinated information sharing and shared security priorities. As stated, the UK already has equivalent cyber security bodies such as those of the EU in place, but the NIS Cooperation Group, which will be created by the NISD will allow for unique mechanisms in the fight against cyber crime. To have the best chance of success, it would be impractical and illogical to exclude themselves from this European cooperation strategy. Nevertheless, it will also be dependent upon what specific agreements come out of the Brexit negotiations.

The crucial point then is for the UK to ensure that negotiations include provisions to continue, if not strengthen, the capacity to harmonise efforts across the EU to tackle cyber risks. This may well be dealt with, at least in part, by the new cyber security laws mentioned in the Queen's speech. Until we know the contents, it is difficult to see whether a stand-alone UK cyber security act will be sufficient, although adoption of the NISD will to a certain extent mitigate these uncertainties. For the remainder, even with

[9]HM Government, 'National Cyber Security Strategy 2016-2012', available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
[10] European Commission, DG Connect, 'The Directive on Security of Network and Information Systems (NIS Directive), 9 May 2017.
[11] Ibid.

the UK a part of the NIS Cooperation Group, effective, accurate and automatic intelligence sharing will not be guaranteed with other key players in the cyber security realm.

3.1 Europol

Europol is at the centre of the EU's approach to fighting international crime. It was created as an intergovernmental organisation in 1995, but converted to EU agency status in 2010. It operationally and analytically supports national law enforcement authorities across the EU in the 28 member states. Europol undoubtedly facilitates cross-border cooperation and help states deal with security threats with a cross border element. Even with the UK's high-level capacity, many areas such as cyber crime are inherently borderless, where several countries are involved. As one example, a server may be located in one country and its many users in another. Therefore technical capacity and sophistication becomes a futile issue, as cross-border information sharing becomes vital. The UK's unrivalled cyber security capacity does not preclude the need for cooperation with other countries. This, together with the fact that approximately 40% of the Europol case load has a British focus, as well as the fact that in 2015, the UK initiated around 2,500 cases for transnational investigation, highlights the sheer importance of Europol.[12]

In 2016, Europol's governance structure changed where the Regulation (EU) 2016/794 aligned Europol's framework[13] with the requirements of the Treaty of Lisbon. These changes took effect on 1 May 2017. The UK in this instance opted into the Regulation as:

> Opting in w[ould] maintain operational continuity for UK law enforcement ahead of the UK exiting the EU, ensuring [that the UK] Liaison Bureau at Europol is maintained, and that law enforcement agencies can continue to access Europol systems and intelligence. This decision is without prejudice to discussions on the UK's future relationship with Europol when outside the EU.[14]

Although this opt-in means continued cooperation with Europol, Brexit will call into question this relationship and form part of negotiating agreements. This is because the opt-in is dependent upon membership of the European Union. There will ultimately be severe dents to the UK-Europol relationship and the ability to tackle cyber crime if a strong cooperative agreement is not entered into.

It is, thus, quite apt here to discuss the issue of Denmark and the situation that arose during a process that eventually led them to signing out of Europol. Whilst not identical to the Brexit issue, Denmark's case provides some insight into the member state and Europol relationship. The country only recently signed a special agreement. This was seen to be a 'backdoor' to Europol cooperation and followed the 2016 referendum in Denmark where most Danes refused full membership of the EU agency. The referendum was prompted by the change of Europol's legal status on 1 May 2017.[15]

---

[12] James Black, Alex Hall, Kate Cox, Marta Kepe, Erik Silfversten, 'Defence and Security after Brexit: Understanding the Possible Implications of the UK's Decision to leave the EU' (2017) RAND Europe.
[13] This is via Council Decision 2009/371/JHA; Regulation (EU) 2016/794.
[14] Letter dated 14 November 2016 from the Minister for Policing and the Fire Service (Brandon Lewis) to the Chair of the European Scrutiny Committee, Sir Wiliam Cash, available at http://europeanmemoranda.cabinetoffice.gov.uk/files/2016/11/Sir_W_Cash_1411161.pdf.
[15] Council of the European Union, 'Declaration by the President of the European Council, the President of the European Commission and the Prime Minister of Denmark to minimise the negative effects of the Danish departure from Europol, following the referendum in Denmark on 3 December 2015, 15 December 2016; 779/16.

The Danish and EU Parliaments voted to allow for the continued participation in the policing and data resource-sharing organisation, a type of relationship that differed from supranational EU legal cooperation. The operational agreement outlined exactly which Europol databases Denmark could access and the procedural steps that Denmark would follow in order to access them. As part of the agreement, Denmark would have observer status, but would be able to allocate Danish officers at Europol with Europol officers placed in Denmark. Whilst this was seen as reducing the adverse effects of departure from Europol, it still means that Denmark will not retain automatic access to crucial information held by Europol, which some say is crucial for cyber security and cannot be mitigated by half-way house type agreements such as this one. Instead, they would be required to communicate requests to Europol staff who would make checks within defined agreement provisions, as opposed to Denmark being able to do this themselves. This would, for one, lengthen the time taken to make these checks and consequently weak capabilities. Furthermore, the agreement meant that Denmark had to continue being a member of the Schengen Agreement.

The Europol Council's initial declaration of Denmark as a third (non-EU) state is extremely unusual, particularly since it was made under the Europol Council Decision of 2009, where Denmark partakes as a full member state. The UK Parliament have themselves questioned why the proposed Council Implementing Decision was imperative, since the wording of Protocol 22 to the EU Treaties on the Position of Denmark and Article 75 of the new Europol Regulation.[16] Nonetheless, despite the UK opt-in, remarks made with reference to the Danish position clearly show that the UK's relationship with Europol will be affected upon withdrawal from the EU. Jean-Claude Juncker, Donald Tusk and the Danish Prime Minister, Lars Lokke Rasmussen, stated in a declaration that

> arrangements must be Denmark-specific, and not in any way equal full membership of Europol, i.e. provide access to Europol's data repositories, or for full participation in Europol's operational work and database, or give decision-making rights in the governing bodies of Europol. However, it should ensure a sufficient level of operational cooperation including exchange of relevant data, subject to adequate safeguards.
>
> This arrangement would be conditioned on Denmark's continued membership of the European Union and of the Schengen area, on Denmark's obligation to fully implement in Danish law Directive (EU) 2016/680/EU on data protection in police matters by 1 May 2017 and on Denmark's agreement to the application of the jurisdiction of the Court of Justice of the EU and the competence of the European Data Protection Supervisor.[17]

The fact that the special agreement, which was entered into was permitted and 'conditioned' due to Denmark's continued member of the EU and Schengen area, infers that a membership (or non-membership as the case may be) status less than this would equal an even lesser agreement than what was entered into between Denmark and the EU.

The UK could and is almost likely to become a third state as far as Europol is concerned, like the United States of America and other – often non-EU – countries, and with a much weaker relationship with the

[16] Protocol 22 to the EU Treaties on the Position of Denmark, 12012E/PRO/22, Official Journal of the European Union, 26 October 2012, C326/1; Regulation (EU) 2016/794 of the European Parliament and of the Council, L 135/53, Official Journal of the European Union, 11 May 2016.
[17] European Commission, Press Release, 'Declaration by the President of the European Commission, Jean-Claude Juncker, the President of the European Council, Donald Tusk and the Prime Minister of Denmark, Lars Lokke Rasmussen, 3 December 2015, available at http://europa.eu/rapid/press-release_IP-16-4398_en.htm

organisation than is currently in place. Here, the UK and Europol would enter into strategic or operational agreements in which particular mutual legal assistance would take place. For example, Europol entered into one of these agreements in 2016 with Ukraine to tackle cross-border crimes such as drug trafficking, counterfeit goods and illegal migration. Iceland, Norway, Switzerland and Liechtenstein are also on the list of third countries as per the Europol Council Decision 2009, but are also associate members of the Schengen free movement zone. Any proposal for a country to be added to the list must be approved by a qualified majority of the Council, as recommended by Europol's management board, as well as the argument that an operational cooperation agreement is necessary.[18]

Once withdrawn from the EU, the UK could enter into two different types of agreements. One is a strategic agreement which focus on the interchange of general data, as well as strategic and technical intelligence. The other type of agreement is an operational agreement, as was done by Denmark. The latter permits the exchange of personal data, but is dependent upon the third state making sure there is sufficient data protection in their country. Unfortunately, the UK will not have the luxury of deciding on the type of agreement. Following the new Europol Regulation, which came into effect from 1 May 2017, the procedure of operation agreements has changed.

Pre-2009, this was solely determined by the Europol's Management Board. However, now, the Commission has implemented an 'adequacy decision' measuring the third state's level of data protection. This already existed, but now has a specific threshold to satisfy before Europol can transmit personal data to established 'third states'. The operational agreement must be concluded via an international agreement with the third country 'adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'.[19]

Since data protection is a key criteria upon which the Board makes it decision, it does place the UK in a good position, given the level of data protection standards that the UK currently possesses and follows, as well as intentions to adopt the GDPR, NISD and generally stronger data protection laws. This will also be measured by Europol's Joint Supervisory Body. The Director of Europol will carry out negotiations supervised by the Board and approved by the Council, as per the qualified majority. Whilst there are various options for the UK, it is unclear of how it will proceed, since there is no status quo on the issue.

3.2 Eurojust

The UK's relationship with Eurojust is also likely to be affected following Brexit. Eurojust assists with the investigation and prosecution of cross-border crime, with significant attention paid to cybercrime.[20]

---

[18] Articles 23 and 26 of Council Decision 2009/371/JHA establishing the European Police Office (Europol), 6 April 2009, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0371&from=EN; Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0935&from=EN

[19] See Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&rid=1

[20] Eurojust, 'Cybercrime on the Rise: A Call for Cyberjustice', available at http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-03-04.aspx.

Their functions include providing advice on the varying law across the EU and facilitating mutual legal assistance between member states. According to Article 86 of the TFEU, Eurojust's mandate is to

> Support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol.[21]

The Eurojust Decision provides a wide-reaching code on data protection and therefore any third country agreements would be subject to the fulfilment of data protection requirements. At the moment, there are a number of cooperation arrangements in place with third countries, such as Norway, Iceland, Ukraine, Montenegro, Moldova, Lichtenstein, Switzerland, Macedonia and the USA.

If these or any other new third countries, such as the UK, fail to meet these requirements, then they would risk losing the ability to cooperate and exchange data with Eurojust. Since the UK already maintains high data protection laws, it is likely that a third country agreement between the UK and the EU would materialise and have the potential to work effectively. The ability to work with Eurojust in real time and establishing Joint Investigation Teams also facilitates effective cooperation and would be imperative for stronger cyber security. This could still be possible as a third country, as the examples of Norway and Switzerland prove. However, these countries' do not have access to other information sharing platforms such as ECRIS. The UK's lack of access to ECRIS[22] would be detrimental to the fight against cybercrime, as virtual crimes can occur in the UK from other member states and this information would be instrumental to the UK for effective cyber policing. Furthermore, since the UK would no longer be a part of the Eurojust management board following Brexit, they would not have the same level of input in the overseeing and development of Eurojust. The organisation could then potentially advance in ways which are not fit for the UK's purpose and context, without the UK's contribution in the matter. This could again be quite detrimental for the UK's continuous strengthening of cyber security, if they are unable to help shape organisations such as Eurojust in line with the types of cyber threats that they are facing the most.

3.3 Mutual Legal Assistance

One option for the UK would be to strengthen the means of cooperation through the use of letters of request, or *Commissions Rogatoires*, which form part of the mutual legal assistance process. States formally collaborate in criminal proceedings and seek help from each other on issues such as the request for procedural documentation, retention of evidence, the freezing/confiscation of assets, the transfer of witness or other evidence, the service of summonses, *et cetera*, as part of cross-border criminal investigations. The mutual legal assistance process is usually triggered by authorities (usually the judiciary) when cross-border cooperation and data sharing does not prove successful in itself. It allows domestic bodies to benefit from actions that they would not normally have the jurisdiction to be a part of, proving its tremendous use in tackling transnational crime, particularly cyber crime.

Currently, as per powers under The Crime (International Co-operation) Act 2003 there stands seven EU agreements reinforcing mutual legal assistance. Whilst police can cooperate on a state-to-state basis via

[21] Article 86 of the TFEU.
[22] Adam Jackson, Gemma Davies, 'Making the Case for ECRIS: Post "Brexit" Sharing of Criminal Records Information between the European Union and United Kingdom' (2017) The International Journal of Evidence & Proof. ISSN 1365-7127.

memoranda of understanding that should remain relatively unchanged after Brexit, the UK's relationship – this includes the UK International Crime Bureau (UKICB) and National Crime Agency (NCA) – with EU agencies that deal with mutual legal assistance will be affected.

Bilateral mutual legal assistance treaties have been created, such as the recent one between the UK and China on criminal activity. There are also multilateral agreements ratified by the UK. For example, the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[23] is an agreement that could be strengthened or replicated on other specifically cyber matters following Brexit. Other similar agreements include the 2003 United Nations Convention Against Corruption (UNCAC)[24]. These are very viable options for the UK within the EU framework to increase its frequency within, although even MLA comes with its own procedural hurdles, as in any domestic regime. Another issue to think about is that under the Crime (International Cooperation) Act, the UK also provides assistance to other requesting countries. This reciprocity could be a crucial card to pull out in negotiations and for other European countries to seriously consider during the negotiation process. The UK could thus enter into creating bilateral or multilateral agreements with each European country or with the EU as a whole. It is apparent though that mutual cooperation is the cornerstone of dealing effectively with cyber crime and cross border crime in general. It is therefore the loss of political goodwill that is the real risk.

4. Concluding Remarks

The UK has always retained one of the highest levels of data protection and will continue to do so following Brexit, particularly given its intentions to adopt the GDPR and NISD. The weaknesses to cyber security will not necessarily be caused by data protection, but rather, the intelligence sharing relationships with EU bodies. Without membership to Europol, it is clear that there would be serious operational gaps and a significant lack of capacity to tackle organised crime and terrorism, and particularly cybercrime, which transcends traditional state boundary lines. The UK must therefore make a suitable agreement that will not deprive them of the instrumental information contained in Europol databases. The Danish model provides a timely alternative, but still highlights the handicap of not fully being a Europol member. Even with sophisticated skills and newly established National Cyber Security Centre, it is no match for fragmented attributes of cross-border crimes, the resolution of which is dependent on interactions with allies and not solely sophistication of technology.

It is vital that if UK want to have the best possible chance of combatting cyber crime, they must not only have access to data held by organisations such as Europol, but also remain close to Eurojust and databases such as ECRIS. Whilst agreements have been made with third countries, such as Norway and Switzerland, these have been conditional upon them being part of Schengen and they have not included automatic rights to ECRIS and other crucial databases such as Prüm and the Second Generation Schengen Information System (SIS II). UK's exit from the EU could have potentially serious implications on its ability to access crucial cyber intelligence. In addition, they would no longer have the same level of contribution to the evolution of these bodies. All of this means that intelligence sharing, which is vital for effective cyber security capacity would be affected. The UK must find a way to keep the current positions as far as the relationships with these organisations are concerned, as well as strengthen mutual legal assistance agreements with the EU.

[23] Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000/C 197/01.
[24] United Nations Convention against Convention, New York, 31 October 2003, Chapter XVIII, Doc. A/58/422.