BINGHAM CENTRE FOR THE RULE OF LAW

appg

APPG on the Rule of Law

Meeting Report:
EU Law, the Investigatory Powers Act, and UK-EU Cross-Border Crime and Security Cooperation

14 March 2017, 17:30-18:45

Room A, 1 Parliament Street

Contents

BIICL

British Institute of International and Comparative Law

Registered Charity No. 209425
Company No. 615025

www.binghamcentre.biicl.org

Format

17:30 – 10:35	**The Rt Hon Dominic Grieve QC MP (Chair)** Introduction
17:35 – 17:50	**3 expert speakers** (5 minutes each)
17:50 – 18:20	**Questions and comment** – MPs and Peers
18:20 – 18:45	**Questions and comment** – open to the floor

Attendance

Chair: The Rt Hon Dominic Grieve QC MP

MPs and Peers: Baroness Hamwee; Baroness Ludford; Lord Anderson of Swansea; Dominic Grieve QC; Mark Durkan MP; Peter Kyle MP; Lord Judd

Others in attendance included: Professor Sir David Omand (Kings College London); Hannah Stone (coordinator, APPG on Extraordinary Rendition); Harmish Mehta; Marek Marczynski (Amnesty International international secretariat); Katie Barraclough (House of Lords Committee Office); Dr Thomas Maguire (King's College London); Darragh Coffey (University of Cambridge); Harry Richardson (Office of Michelle Donelan MP); Carolina Gasparoli (Law Society); Max Hill QC (Incoming Independent Reviewer of Terrorism Legislation); Sir Stanley Burnton (Interception of Communications Commissioner, IOCCO); Eleanor Beeson (Intelligence Services Commissioner's Office); Rosie Slowe (Bingham Centre); Swee Leng Harris (Coordinator of the APPG on the Rule of Law); James Campbell (Bingham Centre)

Meeting Aim

To provide MPs and Peers with an opportunity to discuss the EU's Court of Justice decision in Watson on communications data retention and access, and its implications for the Investigatory Powers Act as well as future UK-EU cooperation on cross-border crime and security.

Background

On 21 December 2016, the EU's Court of Justice (CJEU) held that the indiscriminate and general retention of communications data is incompatible with the privacy protections enshrined in the EU Charter of Fundamental Rights. In light of the CJEU decision, significant features of the UK's Investigatory Powers Act 2016 are probably incompatible with EU law. Despite Brexit, the decision is likely to remain important for UK cooperation with EU partners in the fight against transborder crime and terrorism.

Joined Cases *Tele2 Sverige AB and Watson and Others*

The case challenged retention of communications data under the Data Protection and Investigatory Powers Act 2014 (DRIPA).[1] The case arose out of the CJEU's 2014 Digital Rights Ireland judgment[2] declaring invalid the 2006 Data Retention Directive that imposed a general obligation to retain traffic and location data.[3]

---

[1] Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Watson and Others ('*Watson*')

[2] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others ('*Digital Rights Ireland*')

[3] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in

The CJEU found that DRIPA was inconsistent with the EU Charter of Fundamental Rights privacy protections. The CJEU observed that the communications data:

> taken as a whole, is liable to allow very precise conclusion to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[4]

As such, communications data are capable of 'establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communication.'[5]

In response to the argued necessity of the measure for fighting 'serious crime' and 'terrorism', the CJEU held that this could not in itself justify 'the general and indiscriminate retention of all traffic and location data'.[6] The argued necessity might justify more limited and targeted data retention, so long as the legislation set clear precise rules and effective safeguards.[7]

The CJEU further held that access to retained data should be subject to prior review by a court or an independent administrative authority.[8] Furthermore, persons in respect of which such information is accessed must be notified once the potential to jeopardise the investigations has gone.[9]

Investigatory Powers Act 2016

Whilst DRIPA expired at the end of 2016, the judgment is relevant for the Investigatory Powers Act 2016 (IPA), which similarly provides for data retention for the purpose of preventing crime (not just serious crime - see part 4 of the Act). Compared to DRIPA, the IPA extends both the data covered to include internet use data, as well as the categories of authorisations and warrants that can be sought by governmental authorities to access the data, which do not require judicial approval. [10]

According to Angela Patrick, the impact of the Watson decision may extend beyond IPA's communications data provisions:

> In so far as it confirms the previous case law of the CJEU and the broad approach of the ECtHR to targeting surveillance, strict necessity and safeguards, it may leave a significant part of the Act which avows and provides a statutory basis for "thematic" and bulk surveillance open to challenge.[11]

---

connection with the provision of publicly available electronic communications services or of public communications networks.

[4] *Watson*, at [99]. See also *Digital Rights Ireland, at* [27].

[5] *Watson*, at [99].

[6] *Watson*, at [103].

[7] *Watson*, at [108-109].

[8] *Watson*, at [114].

[9] *Watson*, at [121].

[10] T. Raine, 'The CJEU and Data Retention: A Critical Take on the *Watson* Case', U.K. Const. L. Blog (16 January 2017) (available at https://ukconstitutionallaw.org/).

[11] A. Patrick, 'Who sees you when you're sleeping? Who knows when you're awake?' UK Human Rights Blog (21 December 2016) (available at https://ukhumanrightsblog.com/).

Liberty has stated that it believes the data retention powers are unlawful and is preparing a legal challenge to the IPA.[12]

General Data Protection Regulation

The General Data Protection Regulation, adopted by the EU in 2016, sets out a range of digital consumer rights that protect privacy. The Regulation will be directly applicable in EU countries without the need for domestic implementation. It remains to be seen to what extent IPA is compatible with the Regulation. The Regulation does not apply to the processing of personal data for the purposes of preventing and investigating criminal offences and threats to public security (Article 2(2)(d)). Even where it does apply, data may still be processed without consent where it is 'necessary for compliance with a legal obligation to which the controller is subject' (Article 6(1)(c)) or 'necessary for the performance of a task carried out in the public interests'. However, the requirement that the data be 'limited to what is necessary in relation to the purposes for which they are processed' (Article 5(1)(c) is likely also to preclude the general and indiscriminate retention of data required under the IPA 2016.

What about Brexit?

Although the UK's departure from the EU will mean the UK will no longer bound by EU law, a need for compliance will remain likely. First, the CJEU and European Court of Human Rights in Strasbourg have a practice of referring to each other's case law. This means that it is very likely that the latter court would likewise hold that such national legislation is incompatible with the right to privacy enshrined in Article 8 of the European Convention on Human Rights, to which the UK will remain a party.

Secondly, a practical need for compliance will remain likely if the UK wants to continue to cooperate with the EU, on transborder crime and terrorism. In 2015, the CJEU ruled in the Maximilian Schrems case that non-EU countries must demonstrate "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order"[13] and that the CJEU had jurisdiction to examine whether the transfer of data to a third country is compliant with EU law.[14]

Concerns with the Watson decision

Whilst hailed by many human rights advocates as a great step for the protection of privacy, the decision has not received universal approval. David Anderson QC[15], Anthony Speaight QC[16] and Thomas Raine[17] have

---

[12]Liberty press release statement (21 December 2016) (available at https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/government-breaking-law-collecting-everyones-internet-and-call).

[13] Case C-362/14 Maximillian Schrems v Data Protection Commissioner, at [73].

[14] *Ibid*, at [60]-[61].

[15]D. Anderson, 'CJEU judgment in Watson', Independent Reviewer of Terrorism Legislation (21 December 2016) (available at https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/).

[16] A. Speaight, 'Charter reach extended, national security hampered, EU competence exceeded' Judicial Power Project (11 January 2017) (available at https://judicialpowerproject.org.uk/anthony-speaight-qc-tele2-sverige-charter-reach-extended-national-security-hampered-eu-competence-exceeded/).

[17] T. Raine, 'The CJEU and Data Retention: A Critical Take on the Watson Case', U.K. Const. L. Blog (16 January 2017) (available at

all raised the practical value in terms of law enforcement provided by general data retention powers that the decision undermines.

David Anderson QC argues that access to retained communications data is useful to police both in searching for missing persons and in the fight against serious crime, such as by identifying the true conspirators behind drug trafficking offenses. Moreover, he observes that it is access to the *old* data that in such circumstances is required, both because of a potential time lapse between the incident and the identification of a suspect and because of a decrease in the use of communication channels in the run up to a crime.

Anthony Speaight QC also criticises the decision on the grounds of practicality and law. Speaight draws attention to Art. 4(2) of the Treaty on the European Union, which states that '[n]ational security remains the sole responsibility of each Member States.' Hence, he argues that the Watson decision lies outside the competences of the EU and, whilst curtailing the tools used for finding missing persons and fighting regular crime, should not be followed in respect of the fight against terrorism.

Home Secretary Amber Rudd has stated that she will seek support from other European interior ministers in finding ways around the decision in the effort to combat cross-border crime and terrorism.[18]

Rule of Law

The Watson decision IPA raise a range of rule of law questions, including the following:

- How should technology be used to enforce the law against terrorist or other criminal activity?
- What should the balance be between protecting the right to privacy and use of surveillance and communications data for law enforcement?
- In light of Brexit, what legal framework should the UK adopt to facilitate cooperation with the EU on criminal and security matters?

The Bingham Rule of Law Principles

The rule of law questions above are based on eight rule of law principles that were identified by Lord Bingham, which can be summarised as:

1. The law must be accessible and so far as possible, intelligible, clear and predictable;
2. Questions of legal right and liability should ordinarily be resolved by application of the law and not the exercise of discretion;
3. The laws of the land should apply equally to all, save to the extent that objective differences justify differentiation;
4. Ministers and public officers at all levels must exercise the powers conferred on them in good faith, fairly, for the purpose for which the powers were conferred, without exceeding the limits of such powers and not unreasonably;

---

https://ukconstitutionallaw.org/2017/01/16/thomas-raine-the-cjeu-and-data-retention-a-critical-take-on-the-watson-case/).

[18] H. Warrell, 'UK to press EU for loopholes in surveillance ruling', Financial Times (25 January 2017) (available at https://www.ft.com/).

5. The law must afford adequate protection of fundamental human rights;
6. Means must be provided for resolving without prohibitive cost or inordinate delay, bone fide civil disputes which the parties themselves are unable to resolve;
7. Adjudicative procedures provided by the state should be fair; and
8. The rule of law requires compliance by the state with its obligations in international law as in national law.

Speakers' Summaries

Jessica Simor QC

Please see attached annex.

David Anderson QC: CJEU judgment in Watson

The following is based on David Anderson QC's post on the Independent Reviewer of Terrorism Legislation, which can be viewed in full at https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/

What are the powers in issue?

The power of chief concern to the Court was the power to require communications service providers to retain fixed and mobile call logs ("traffic data") and mobile phone location data for up to 12 months.

Those powers have been exercised in the UK for many years. The EU's own Data Retention Directive of 2006, a measure supported by the UK Government which required such powers to be exercised EU-wide, was itself struck down by the Court in 2014 (*Digital Rights Ireland*). Many Member States have continued to exercise such powers under their own national law, and a number of them (Czech Republic, Cyprus, Estonia, Finland, France, Germany, Ireland, Poland) joined the UK in arguing in this case that the principles set out in *Digital Rights Ireland* should not be treated as mandatory requirements in these circumstances.

What are the powers used for?

The DRIPA 2014 power at issue in *Watson* is a relatively familiar and low-tech one: contrast some of the bulk collection powers used by security and intelligence agencies in the UK and other countries whose utility I reviewed in this report of August 2016. (The Treaty on European Union states at Article 4(2) that "*national security remains the sole responsibility of each Member State*": the scope of that carve-out remains to be definitively determined.)

Access to retained traffic and location data is however extremely useful to the police and other law enforcement authorities, in the investigation not only of serious crime but e.g. of reported disappearances where examination of the phone records of the missing person may offer clues as to their contacts and so help locate them. During my investigatory powers review of 2014-15, I was left in no doubt as to its value.

Some specific examples of the utility of retained communications data in investigating both missing persons and serious crimes (sexual offences, supply of drugs, trafficking, homicide, terrorism) are at Annex 10 to my June 2015 report, A Question of Trust. Similar examples were provided to the European Commission from a variety of Member States. See further A Question of Trust at 7.47-7.51, 9.21-9.32 and 9.43-9.47. As I wrote at 9.45, retained data may be particularly useful because:

- Conspirators become more guarded in their use of communications as the moment of a crime approaches. Older data may therefore be the best evidence against them.
- It may be relatively easy to arrest the minor players in a drugs importation or smuggling ring. But by going through their historic communications data, it may become possible to trace the bigger players who have taken care to remain in the background.
- A time lapse between the incident and the identification of a suspect will mean that old data is needed.

Law enforcement figures cited at 7.50(c) showed that over a two-week period in 2012, 27% of requests for communications data in terrorism cases and 37% of requests in sexual offence cases were for data more than six months old.

I also quoted Rob Wainwright, the (British) Director of Europol, who gave the following evidence to the European Parliament in late 2014:

"Ask yourself what the end of data retention would mean in concrete terms? It would mean that communications data that could have solved a murder or exonerate a suspect is simply deleted and no longer available."

The European Commission has been a strong supporter of universal retention of communications data, noting in 2014:

"Data retention enables the construction of trails of evidence leading up to an offence. It also helps to discern or corroborate other forms of evidence on the activities of and links between suspects and victims. In the absence of forensic or eye witness evidence, data retention is often the only way to start a criminal investigation. Generally, data retention appears to play a central role in criminal investigation even if it is not always possible to isolate and quantify the impact of a particular form of evidence in a given case."

Precisely because suspects are often not known in advance, data retention which is not universal in its scope is bound to be less effective as a crime reduction measure. In addition, a person whose data has not been retained cannot be exonerated by use of that data (e.g. by using location data to show that the person was elsewhere).

The judgment: minimum safeguards

The Court followed its Advocate General (the member of the court entrusted with preparation of a preliminary opinion) in requiring that access to stored data should be restricted to serious crime purposes (para 119) and subject to prior independent authorisation (para 120). Those points were anticipated also by the English High Court in its ruling of July 2015, though on grounds which were doubted by the Court of Appeal in November 2015.

The judgment also introduced a requirement to notify persons affected when such notification is no longer liable to jeopardise an investigation (para 121). It further requires that data must be retained in the EU (para 122: this is not currently the case for all data).

The judgment: principle of general data retention

The wider significance of the Grand Chamber's judgment is in its ruling that the whole principle of what it called *"general and indiscriminate retention"* (para 97) is contrary to EU law – specifically the Charter of Fundamental Rights.

…

The judgment of the CJEU was thus a genuinely radical one. The proven utility of existing data retention powers, and the limitations now placed on those powers, is likely to mean that it will be of serious concern to law enforcement both in the UK and in other Member States. On the other side of the balance, not everyone will agree with the Court's view that these powers constitute a "*particularly serious*" interference with privacy rights, or that they are "*likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance*" (para 100). A more rigorous analysis of proportionality would have focussed on any actual harm that this useful power might be shown to have caused over its years of operation, and sought to avoid assertions based on theory or on informal predictions of popular feeling.

It must be acknowledged, however, that feelings on these matters do vary at least to some extent across Europe. Thus:

- The comments of the CJEU in relation to the seriousness of the interference with privacy find no real echo in the three parliamentary and expert reports which led to the introduction of the Investigatory Powers Bill, nor in the regular reports of the Interception of Communications Commissioner, the senior former Judge who conducts detailed oversight of this activity in the UK.
- But in the eastern part of Europe and in Germany, historic experience, coupled with a relative lack of exposure (until recently) to terrorism have induced greater circumspection. National data retention rules have proved controversial and were annulled even before *Digital Rights Ireland* in Bulgaria, Romania, Germany, Cyprus and the Czech Republic.

This may reflect what I have previously described as "*marked and consistent differences of opinion between the European Courts and the British judges … which owe something at least to varying perceptions of police and security forces and to different (but equally legitimate) conclusions that are drawn from 20th century history in different parts of Europe*" (A Question of Trust, 2.24).

Geographical profiling?

The qualms expressed by the Court in relation to the principle of universal data retention did not extend to a retention obligation "*based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences …*". Indeed the CJEU advised that:

"*Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences*" (para 111).

Did the Court mean by this that it could be acceptable to perform "*general and indiscriminate retention*" of data generated by persons living in a particular town, or housing estate, whereas it would not be acceptable to retain the data of persons living elsewhere? Such geographical profiling could prove "*wholly impracticable*", in the phrase of Dinah Rose QC. If attempted, it would certainly raise extremely sensitive legal and ethical issues. Those issues were not touched upon in the judgment.

Bella Sankey: Liberty's challenge to the Investigatory Powers Act 2016

Liberty has recently issued a legal challenge to the Government's landmark surveillance legislation, the Investigatory Powers Act 2016. The challenge is being crowdfunded via CrowdJustice, and has received widespread public support. More than 200,000 people signed a petition calling for the Act's repeal after it passed late last year.

The Act creates the most intrusive legislative surveillance framework of any democratic country in history. The powers we're fighting undermine everything that's core to our freedom and democracy – our right to protest, to express ourselves freely and to a fair trial, our free press, privacy and cybersecurity.

Liberty is challenging the unprecedented "bulk" surveillance powers contained in the Act on the grounds that these powers are in breach of Articles 7 & 8 of the EU Charter of Fundamental Rights & Freedoms and Articles 8 & 10 of the European Convention on Human Rights. Liberty will argue that the following powers breach the British people's rights:

Bulk and 'thematic' hacking
The Act lets police and agencies access, control and alter electronic devices like computers, phones, tablets smart TVs on an industrial scale, regardless of whether the interference is linked to a criminal investigation, or prevention of a specific crime. While State hacking may be justifiable if used in a highly targeted manner, and strictly monitored, indiscriminate hacking undermines digital rights and risks our cyber-security, leaving potentially millions of devices compromised and vulnerable to further attack by hackers.

Bulk interception of communications content
The Act lets the state read texts, online instant messages and emails, and listen in on calls en masse, without requiring suspicion of criminal activity.

Bulk retention and acquisition of communications data and internet histories
The Act forces communications companies and service providers to retain and hand over records of everybody's emails, phone calls and texts and entire web browsing history to state agencies to store, data-mine and profile at its will. This power acts to chill the work of activists, whistleblowers, journalists and public interest lawyers.

Bulk personal datasets
The Act lets agencies acquire and link vast databases held by the public or private sector. These contain details on religion, ethnic origin, sexuality, political leanings and health problems, potentially on the entire population – and are ripe for abuse and discrimination.

Watson
Liberty represented Tom Watson MP in his challenge to the Data Retention & Investigatory Powers Act 2014 (DRIPA); the precursor to the IPA. In December 2016, the CJEU handed down judgment in this case and held that the UK's blanket and indiscriminate data retention provisions breach the Charter of Fundamental Rights.

The judgment mirrors the jurisprudence of the Strasbourg Court, which holds that signatory States' surveillance legislation contains safeguards which ensure that monitoring is individually targeted; based on reasonable suspicion of criminality and authorised in advance by an independent body. Notwithstanding Brexit, the UK will be required to comply with this jurisprudence in by virtue of the European Convention on Human Rights to which the UK will remain a party.

Conclusion
The CJEU judgment effectively renders significant parts of the IPA unlawful. The Act now requires urgent amendment to bring it in line with the Rule of Law and the UK's human rights obligations.

Key Points from Discussion

CJEU Reasoning in Watson

The CJEU's reasoning in Watson was discussed in some detail. One view was that the CJEU was not making 'new' law in its Watson decision, which is based on the 2002 Directive that prohibits data retention The 2006 Directive was directly in contradiction with the 2002 Directive, as observed in *Digital Rights Ireland*. EU law provides a right to data protection under Art 16 TEU and Art 7 of Charter (unlike the European Convention on Human Rights, which does not provide such a free standing right).

Others were critical of the CJEU decision in Watson. The nature of the CJEU's proportionality exercise was shoddy, and the nub of judgement on why law enforcement agencies are precluded from using the powers in question was insufficient. The decision was put on basis of 'feeling' that one's private life is under constant surveillance, and lacked nuanced and informed discussion of how the powers are used. Courts need to decide these cases based on the evidence on how these powers are used, and States need to be more forthcoming with information on how the powers are used.

Some took the view that safeguards on access to data was a better approach than constraining data retention, as retention is not a problem where there are adequate safeguards on access. The CJEU could have followed the approach of the Advocate General, which would not have posed such restrictions on the retention of data. Instead, the CJEU's suggestion of limiting data retention to geographical areas indicates a lack of understanding of the powers. In particular, the CJEU appeared to be unaware of the possible proper uses of the data.

National Security and National Responses to CJEU Decision

The application and operation of Art 4(2) which excludes national security from the TEU remains an unresolved point. In a current case in the UK on bulk personal data sets, Mitting J has asked for arguments on the jurisdiction of the CJEU in light of Art 4. This could even result in another reference to CJEU to resolve the question. The Watson decision prevents bulk data retention, which could mean there are 'parallel worlds' of law enforcement versus national security. And if that is the case, where does terrorism sit?

National security is explicitly excluded in the recitals to the EU Directives. The problem is that data protection as a concept means protection from both private individuals and the state. So there is a contradiction in the concept, and neither of the Directives limit data retention to national security. The UK argued the national security exception in Watson, but had that argument succeeded the 2002 Directive would have been robbed of effect. The national security side of things has effectively been quietly forgotten in order to enforce data protection.

In the context of Watson, Germany had similar argument to Open Rights. France is now in state of emergency and so it may fall within the state of emergency derogation that is permitted under law. In any case, there is speculation that some countries are not intending to comply with the Watson decision, or to route all data through security agency based on the interpretation that an exclusion applies to the activities of any security agency.

The UK Government was criticised for seeking power for national security under the EU, but not accepting rights protections under EU law. It was argued that the Blaire Government used EU law to avoid complexity in UK law.

Oversight and the Law Enforcement and Security Agencies

The careful approach of law enforcement and security agencies was highlighted. For example, at a conference of the 'single points of contact' all of the single points of contact were keen to have guidance on the limits on powers and what is permitted. Each use of powers under the Regulation of Investigatory Powers Act is scrutinised by the relevant single point of contact. The experience of oversight bodies suggests that misuse of powers is usually due to mistake, and never deliberate. There was only one case where data was sought for journalist sources, and the police person in charge was disciplined. The oversight bodies for investigatory powers do not find use of the powers for ulterior purposes. Regardless of the potential for misuse of investigatory powers, the agencies do not in fact misuse the powers. Furthermore, there are oversight bodies that carry out functions that balance the risk of misuse of powers.

However, the arguments for comprehensive accountability and scrutiny are not based on allegations of misuse of powers, rather based on the principle that the law should be clear and accessible. Nor is there underlying criticism of the oversight functions, but the oversight is sufficient because it is not possible to scrutinise all warrants.

Furthermore, the Watson case concerns the requirements imposed by Government on private companies. If case concerned State actions, the Directive would not have been relevant, but the Data Retention and Investigatory Powers Act concerns data retention by private companies. Surveillance carried out directly by the State would be dealt with Arts 7 and 8 of Charter.

Government Overreach

There was discussion of current litigation and confused state of the law being a consequence of governments being over-ambitious and disregarding objections in relation to data retention. It was argued that the Data Retention Directive had been pushed through the EU Parliament in 2005, and had been too broad and lacking sufficient safeguards. The 2005 Directive allowed for derogation from derogation with regard to the 2002 Directive on the confidentiality of data.

It was suggested that the UK had attempted to make a power grab through EU law in the area when the UK held the presidency of the EU. This was compounded by the UK Government's ramming through replacement legislation after the *Digital Rights Ireland* decision, without sufficient processes or scrutiny. It was hoped that the Watson decision would prompt a more considered approach by the UK Government.

Culture and History

There was some shared consensus on the different histories and cultures of European nations being important context for debate on privacy and investigatory powers. The area of investigatory powers is difficult in Europe because there is a large number of countries with different histories and contexts. The 2006 Directive has highly controversial in Eastern Europe and six national courts set it aside. The collection of data in Poland and Hungary is different to the context in the UK, although things could change in the UK. Furthermore, the single data market of the Europe means that these issues are difficult and no longer limited to borders.

Law and Technology

The Digital Economy Bill before Parliament includes provisions on data sharing, for which the issues echoed the debates on the Investigatory Powers Act. Many members of the public may think it is reasonable for Government departments to share data, but the language in the Digital

Economy Bill raises concerns due to its vagueness, for example, 'contribution to society' or 'anti-social behaviour'. The Bill allows the connecting together of bulk data sets, and some view the terminology and gateways in the legislation as troubling.

The underlying issue is that regulation always lags behind technology. Understandably companies and Government want to use data in their activities, but careful thinking is needed on where such broad access to data can lead and what checks and balances are needed.

There was a question on whether the Investigatory Powers Act would hamper obtaining an adequacy decision by the EU Commission after the UK's exit from the EU. The view in response was that the use of investigatory powers may cause difficulty, but such difficulty was not due to the Act itself. Furthermore, the perception in Europe and US is that there is a need for judicial scrutiny of the use of investigatory powers, and it is clear from Watson the CJEU does not like bulk powers.

The Investigatory Powers Act was praised for making investigatory powers accessible and foreseeable, e.g. equipment interference powers. Other countries such as Canada and Germany do not provide for these powers in the laws, but that does not mean the powers are not used in those countries. By contrast the Investigatory Powers Act sets the powers out transparently, allowed Parliament to debate the powers, and citizens to know the powers. The Intelligence and Security Committee had been concerned by the previous Act in terms of the accessibility and foreseeability of the law. The Investigatory Powers Act improved on these concerns and was thus a remarkable achievement.

Speakers Biographies

Jessica Simor QC
Jessica Simor QC is a barrister and founding member of Matrix Chambers, where she specialises in EU and public law, with particular expertise in human rights law. She has previously worked in the European Commission in Brussels (1993), the European Court of Human Rights in Strasbourg (1995-1996) and as legal adviser to the Human Rights Ombudsman in Bosnia (1997). From 2010, she served as a member of the Attorney General's A Panel of Counsel, having previously served on the B and C panels. She represented Privacy International and Open Rights Group in their intervention in the Watson case.

David Anderson QC
David Anderson QC is a barrister at Brick Court Chambers specialising in EU, public and human rights law. Previously, he worked at Covington & Burling in Washington DC (1985-86), the European Commission in Brussels (1987-88) and as a recorder for the South Eastern Circuit (2004-2013). He has been a Visiting Professor at the King's College London since 1999, and is a Judge of the Courts of Appeal of Jersey and Guernsey. Until recently, he served as the Independent Reviewer of Terrorism Legislation (2010-2017).

Bella Sankey
Bella Sanky is the Director of Policy at Liberty, leading Liberty's policy development and parliamentary work aimed at putting human rights matters at the forefront of policy making across the UK. Prior to joining liberty, she worked for the Commonwealth Secretariat and was called to the Bar in 2008.

APPG Rule of Law meeting 14 March 2017 5.30pm

JESSICA SIMOR QC[19]

C-698/15 S/S for the Home Department v Tom Watson and others, Open Rights Group, Privacy International and The Law Society of England and Wales; Cases C-203/15 Tele2 Sverige AB v Post- och telestyrelsen

Joined cases – Swedish case and UK case

Both concerned the compatibility with EU law of national regimes (UK and Swedish) which imposed on providers of publicly accessible electronic communications services an obligation to retain data relating to electronic communications in relation to all means of communication and all users. Essentially, the cases concerned two issues:

> first, whether there were any circumstances in which a general data retention obligation imposed on private telephony service providers by Member States was lawful under EU law, and
>
> secondly, if so, what safeguards, including controls on access were necessary to render that general data retention obligation lawful?

Joined Cases C-293/12 Digital Rights Ireland and C-594/12 Kärntner Landesregierung; Michael Seitlinger, Christof Tschohl and others

The cases followed on from the case of, *Digital Rights Ireland*, in which the Court of Justice in Luxembourg (the CJEU) struck down the EU Data Retention Directive 2006/24 as unlawful under the Treaty because it was in breach of Articles 7, 8 and 52 of the Charter of Fundamental Rights.

The EU Data Retention Directive compelled all ISPs and telecommunications service providers operating in Europe to collect and retain a subscriber's incoming and outgoing phone numbers, IP addresses, location data, and other key telecom and Internet traffic data for a period of six months to two years. It was then to be made accessible to Member States in accordance with the provisions of that Directive.

It was challenged in Austria and Ireland, both cases resulting in a reference to the Luxembourg Court where the legality of the Directive could be determined.

The Court held that data retention "*entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data*" and that it "*entails an interference with the fundamental rights of practically the entire European population*". Accordingly, it struck down the Directive as contrary to the Treaty.

The Court did not accept that such a wholesale derogation was permissible and was in no doubt that the retention of communication data, even if no content was retained, constituted an interference in private life and data protection, as guaranteed by Articles 7 and 8 of the Charter: paragraphs 33-34. In this regard, it took the view that access to such data by "the competent national authorities", constituted an *additional* interference: paragraph 35. The Court, considered the interference particularly grave because of the vague sense of surveillance to which it potentially gave rise and the possibility that this could impact on individuals'

[19] Barrister, Matrix chambers and Lead Counsel with Ravi Mehta (Blackstone chambers) for Privacy International and Open Rights Group.

freedom of expression. As the AG stated at paragraphs 52 and 72 of his Opinion, to which the Court referred at paragraph 37:

> 52. First of all, it is true that it must not be overlooked that the vague feeling of surveillance which implementation of Directive 2006/24 may cause is capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information and that an interference with the right guaranteed by Article 11 of the Charter therefore could well also be found to exist….
>
> 72. …the fact remains that the collection and, *above all, the retention*, in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, *even if* they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives…."

The Court had no doubt that the objective of the legislation was legitimate; to contribute to the fight against serious crime and thus, ultimately to security': paragraph 41-44. As to necessity and proportionality, the Court considered that in light of the matters at issue, namely privacy and data confidentiality, the discretion available to the EU was reduced and its review should be strict: paragraph 48.

As regards retention, the Court applied a strict necessity test in determining the legality of the legislation by reference to its earlier case law: paragraph 52.[20] Thus, the Court noted:

> "Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99).
>
> 55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

The Court noted that the retention obligation was universal, covering all data without regard to any individual characteristic and thus "entail[ed] an interference with the fundamental rights of practically the entire European population": paragraphs 56-59. In that regard the Court noted that its coverage, being comprehensive, meant that it applied even to those subject to rules of professional secrecy: paragraph 58.

[20] The Court cited paragraph 39 of Case C-473/12 *IPI* : "According to settled case-law, the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C‑73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I‑9831, paragraph 56, and Joined Cases C‑92/09 and C‑93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I‑11063, paragraphs 77 and 86)."

As regards, access, the Court held that the legislation failed to provide any objective criteria by which to determine the limits of access by competent authorities. Nor did it contain procedural or substantive safeguards in relation to access: paragraphs 60-61. As the Court noted:

> "62…Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

As regards the retention period, the Court noted that the minimum retention period of 6 months existed without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned: paragraph 63. Nor did it state the basis on which it could be for a longer period or specify the need for objective criteria in order to ensure that it is limited to what is strictly necessary: paragraph 65.

Finally the Court expressed concern that the legislation did not require the data to be retained in the EU, such that the protection of an independent authority guaranteed by Article 8(3) of the Charter was not fully ensured.

For the above reasons, the Court found that the legislation did not comply with the principles of proportionality as required by Articles 7, 8 and 52 of the Charter, such that there was no need for it to go on and consider Article 11: paragraph 70.

The consequence of the CJEU finding that the EU Data Retention Directive was invalid was that the domestic laws, which gave effect to it in Member States, were necessarily called into question and likely unlawful.

The UK response to Digital Rights Ireland: DRIPA

The United Kingdom responded to the striking down of the Data Retention Directive by urgently adopting new legislation to replace the legislation that had implemented it: Data Retention (EC Directive) Regulations 2009 ("2009 Regulations") (C/21/183). The new legislation: the Data Retention and Investigatory Powers Act ("DRIPA"), which provided for its own repeal on 31 December 2016, allowed the Secretary of State by way of Notice to require service providers to retain data. It was that legislation that was challenged by David Davis and Tom Watson.

The basis for the Davis and Watson challenge

The original basis for the challenge to DRIPA was that the legislation was contrary to the Charter of Fundamental Rights. Davis and Watson did not challenge the general retention obligation in itself. Rather they argued that in so far as access to the retained data was not subject to prior judicial authority, it was unlawful.

Open Rights Group and Privacy International argued however, that the general data retention obligation was on its own unlawful, irrespective of any safeguards in relation to access. The basis for that argument was the prohibition on retention of data provided in legislation adopted by Member States to protect individual privacy rights in the context of electronic communications data, namely, Directive 2002/58:

> "for the purposes of harmonizing national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communication equipment and services within the Community": Article 1(1)

It provides that Member States are obliged to ensure the confidentiality of communications and to prohibit, listening, tapping, storage or other kinds of interception or surveillance, except where such interferences are legally authorized in accordance with Article 15(1): see Article 5(1).

Importantly, it contains: (1) a prohibition on data retention: Article 5; and (2) an obligation to ensure that CSPs erase traffic data when it is no longer needed for the purpose of the transmission of the communication: Article 6. The only exception to this is where in so far as necessary the provider of the communication serve may retain traffic data:

a. for billing purposes but only up until the last date on which the bill may be challenged or payment pursued end of the billing period As regards retention: 6(2);

b. may use data for marketing but only if the individual has given his consent: 6(3);

As to identification of numbers, the CSP is obliged to provide a possibility for the user to prevent caller identification: Article 8. As to location data, this can only be processed on an anonymous basis unless the user has given his/her consent: Article 9.

Article 15 permits Member States however, to adopt legislation to restrict the scope of these rights: the right to confidentiality of communications (Article 5); the right to erasure of traffic data (Article 6), the right to non-identification of caller (Article 8) and the right to anonymisation of location and other traffic data (article 9). But such a restriction is only permissible where it:

> "constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the communications system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union [which applies to the Charter to EU law]."

In *Digital Rights Ireland* the Court had noted that the Data Retention Directive was a derogating Act; it had sought to derogate from the derogating provision in Article 15 of Directive 2002/58: see paragraph 32, which refers to the AG's analysis at paragraphs 39-30 of his Opinion. Indeed, it actually amended Article 15 of Directive 2002/58 to add a new paragraph stating that Article 15(1) did not apply in respect of it.

The Decision of the Court

In light of the fact that the CJEU had not accepted an EU measure (the Data Retention Directive) that sought to derogate in full from a prohibition, or put another way negate a prohibition through new legislation, it was perhaps unsurprising that the CJEU was equally not willing to accept a Member State doing the equivalent by way of national legislation. Put simply if it was unlawful for the EU (by way of the agreement of the Member States in Council) to adopt such legislation it was hardly going to be lawful for Member States to do so.

The Court emphasized that a generalized retention obligation allowed precise conclusions to be drawn about someone's private life – 'profiling'. This it considered involved a far-reaching interference with privacy rights, which was particularly serious. The fact that there was no notification had, in the Court's view, the consequence of leading individuals to feel they were under constant surveillance. Whilst accepting that the effectiveness of the fight against serious crime, in particular organised crime and terrorism, "*may depend to a great extent on the use of modern investigation techniques*", the Court considered that "*such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 51)*." In that regard, it noted that Directive 2002/58 requires the retention of data to be the exception, which was necessarily contrary to wholesale indiscriminate retention of data.

The Court was critical of the comprehensive nature of the retention regime, affects all persons using electronic communication services, even though they are not even indirectly, in a situation that is liable to give rise to criminal proceedings. It further noted that there was not even an exception for persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

The Court noted that the legislation required no relationship between the data that had to be retained and a threat to public security. In that regard, the Court noted:

> "In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 59)."

For those reasons, the Court concluded that the national legislation exceeded the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

Finally, however, the Court noted:

> "that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary."

It went on to explain what this entailed:

> "109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 54 and the case-law cited).

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."

Accordingly, by its judgment in *Watson*, the CJEU confirms that EU law precludes national legislation that prescribes the general and indiscriminate retention of data and sets down the criteria for lawful data retention provisions.

The Investigatory Powers Act ("IPA")

The powers in IPA are built on the same model as its predecessor and provides for broad powers of data retention with limited provision for safeguards of the kind that the Court considered crucial. Significant parts of that newly minted legislation lay open to challenge.

Part 3 of the IPA provides for the retention of communications data on a model broadly mirroring DRIPA. The range of bodies which can access data and the purposes for which information can be accessed are slightly narrower, but still clearly wider than that envisaged by the CJEU (see Sections 61(7), 70 and Schedule 4). Section 61(7) still includes functions far wider than serious crime, including public health, taxation and the functioning of financial markets. Retention of data is similarly unconstrained (Section 87). There is no provision for prior judicial authorisation of access to data, except by local authorities. Section 76 replicates the "single Point of Contact" model which sees access decisions authorised internally, subject only to after-the-event scrutiny by the new Investigatory Powers Commissioner, who will not examine all access requests, but may dip-sample or audit on another selective basis.

The decision in *Watson* therefore makes it unlikely that the communications data model in the new legislation is lawful under EU law.