A First Look at the Constitutional and Legal Implications of the Data Retention and Investigatory Powers Act 2014

scripted

Volume 11, Issue 3, December 2014

A First Look at the Constitutional and Legal Implications of the Data Retention and Investigatory Powers Act 2014

Judith Rauhofer, Wiebke Abel, Ian Brown

DOI: 10.2966/scrip.110314.320

1. Introduction

On 17 July 2014, the UK Parliament adopted the Data Retention and Investigatory Powers Act 2014[1] (DRIPA) after the government tabled its initial proposal just a week earlier[2]. DRIPA replaces the Data Retention (EC Directive) Regulations 2009[3], which transposed the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications, services, or of public communications networks, and amending Directive 2002/58/EC (Data Retention Directive)[4] into UK law. The Court of Justice of the EU had declared the Directive invalid on 8 April 2014[5]. As a result, national legal instruments implementing it were highly vulnerable to judicial review.

The UK government introduced DRIPA using the emergency legislative procedure. This meant that the proposal was rushed through parliament with little to no legal scrutiny.

In response to these developments, Judith Rauhofer from the Centre for IP and Technology Law (SCRIPT) at the University of Edinburgh together with Ian Brown from the Oxford Internet Institute at the University of Oxford organised a Workshop on the Data Retention and Investigatory Powers Act 2014 (DRIP workshop) in London on 28 July 2014.

2. Workshop Summary

The workshop was a unique, one-off meeting of interdisciplinary European experts from academia, industry, regulators, policymakers and civil society and was aimed at analysing and assessing the constitutional and legal implications of the new Act.

It consisted of three sessions of formal presentations in the morning followed by parallel unconference[6] sessions for academics and civil society organisations in the afternoon. The aim of the unconference sessions was to determine future steps and potential cooperation between the different groups. While the civil society group discussed next steps in terms of campaigns and judicial review of DRIPA, the academic group set out to identify; areas where academic research was necessary; suitable opportunities for collaboration with civil society and policymakers; and the type of expertise required.

---

[1] The Data Retention and Investigatory Powers Act 2014, available at http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf.

[2] The Data Retention and Investigatory Powers Bill 2014, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/329785/Provisional-DRR2014-with-cover-sheet.pdf.

[3] SI 2009/859, available at http://www.legislation.gov.uk/uksi/2009/859/contents/made.

[4] OJ L105/54.

[5] Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärntner Landesregierung). For a review of the CJEU's decision, see also J Rauhofer and D Mac Sithigh, "The Data Retention Directive Never Existed", (2014) 11:1 SCRIPTed 118, available at http://script-ed.org/?p=1480#_ftn3.

[6] For an explanation of what an unconference is see: WhatIs.com; "unconference" at: http://whatis.techtarget.com/definition/unconference.

This report provides an overview of the issues addressed, highlighting the success of the workshop in terms of generating discussions, and identifying imminent and future action points and aims for collaboration. Over the course of the workshop, several commonly shared concerns became apparent providing a base from which further actions can be taken (as a group as well as individual effort).

3. Workshop Objectives

The DRIPA workshop was intended to advance the (academic) debate on DRIPA by bringing together experts from different fields that would not otherwise have had the opportunity to engage in such discussions. As a one-off and ad-hoc response to the UK government's largely unexpected, controversial, and rushed policy actions the main objectives were; to establish a shared knowledge base; define the most pressing constitutional legal issues raised by the new act; initiate collaboration among the attendees; and develop ideas for future collaboration. Based on these overarching aims, the workshop organisers had set out a number of questions to guide and inform the discussions.

In particular, they asked:

- To what extent the new data retention provisions contained in DRIPA were compatible with the principles for fundamental rights compliance set out by the CJEU in its decision on the Data Retention Directive.
- For clarification of new provisions contained in section 4 of DRIPA relating to the extraterritorial application of the interception provisions contained in the Regulation of Investigatory Powers Act 2000 (RIPA)[7].
- To what degree DRIPA impacts on communication service providers (CSPs) that provide pan-European services but route communications via the UK and hold data in the UK.
- What procedural and EU/UK constitutional issues arise from DRIPA and the emergency procedure approach, including compliance with the EU notification procedure under the EU Transparency Directive (2004/109/EC) and judicial review.

The sessions were arranged according to these overarching aims with expert speakers giving short talks on the identified issues and plenary discussions following these.

Aside from this loosely pre-defined structure and aims, the workshop agenda was deliberatively kept flexible to enable as much discussion as possible, and encourage cooperation between the different groups.

4. Workshop Presentations and Activities

The workshop was opened by Ian Brown and Judith Rauhofer with a short overview of the agenda and introduction to the topic. To increase the openness of the discussion and to enable a free and frank exchange of views the workshop was held under the

[7] The Regulation of Investigatory Powers Act 2000; available at http://www.legislation.gov.uk/ukpga/2000/23/contents.

Chatham House Rule. This report will therefore not include direct quotes or attribute statements to individual speakers except where they gave specific permission.

4.1 Reactions to and implementation of the CJEU decision

Panellists: Dr TJ McIntyre (Digital Rights Ireland) and Prof. Franziska Boehm (University of Münster)

This panel focused on the decision of the CJEU to declare the Data Retention Directive invalid, and the impact of this decision on the law of the member states.

TJ McIntyre, a director of Digital Rights Ireland, one of the claimants in the case, gave an overview of the proceedings culminating in the CJEU judgment in April 2014. While the challenge to the Directive dated back all the way to its adoption in 2006, he expressed the view that the revelations of Edward Snowden about the surveillance practices of the NSA and other national security services had had a huge impact on the court proceedings and the ruling. Describing the oral hearing, he noted that the judges had made an unprecedented effort to understand the technical aspects of data retention and had clearly studied the relevant technical issues at stake.

McIntyre explained that it had been a once in a generation chance to litigate these issues just after the Snowden revelations, where the court was aware of the significance of the topic and was willing to engage in-depth with the relevant technical issues. Given the limited ways in which a case can be brought before the CJEU, it does not happen often that the court is available to address these types of issues. McIntyre noted that despite the fact that many national laws on data retention were struck down before the Data Retention Directive was declared invalid,[8] national courts are nonetheless often reluctant to refer issues to the CJEU. On this occasion, a piece of legislation that caused much disturbance Europe-wide took seven years to be heard by the court. There is at least a possibility that without the Snowden revelations, the case would not have been heard at all. The huge public impact of these revelations was therefore a unique opportunity.

Franziska Boehm, who together with Mark Cole from the University of Luxembourg had just prepared a study[9] on data retention after the CJEU judgment, focused on the impact of that judgment. She emphasised that it does not happen often that a piece of legislation is declared void in its entirety and that this will have a significant impact on existing data retention measures. Member states will have to react and consider the judgment and it may also have an impact on other EU Directives, in particular Directive 2002/58/EC on privacy and electronic communications (E-privacy Directive). Additionally, the court's decision might impact on other regimes including, most notably, the existing and future agreements between the EU and the US on data exchange (including measures relating to financial transaction data, passenger names records, the planned data protection umbrella agreement and the safe

[8] In the Czeck Republic, Germany and Romania data retention legislation was declared void by the highest courts.

[9] F Boehm and M Cole, "Data Retention after the Judgement of the Court of Justice of the European Union", 30 June 2014; available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

harbour agreement). Some measures currently discussed are much more privacy invasive than the provisions of the data retention directive struck down by the court. This court's decision might therefore become an impetus for renegotiating these measures, and for NGOs to bring further challenges before the courts. Boehm argued that the EU has to at least review existing measures.[10]

Boehm also highlighted that some of the CJEU judges reportedly wanted data retention to be declared unacceptable as such. However, they could not achieve a majority. Boehm reasoned that this posed the question in how far fundamental rights are protected by the judgment from violations through data retention measures. If no "recipe" for the development of lawful measures is provided, member states are potentially given a significant margin of appreciation to adopt new, potentially infringing, data retention laws that may then be open to fresh legal challenges. Nevertheless, Boehm stressed that the judgment is unprecedented in detail and very specific, particularly from an EU perspective.

Boehm concluded with the observation that DRIPA must be seen in the wider EU context where the CJEU is still in the process of developing coherent case law on data protection issues. One of the main reasons for the enactment of the Data Retention Directive was the failure of many national parliaments to adopt similar measures. Therefore, the judgment should be analysed in the context of the CJEU's decision in the case of the Google Spain judgment[11] to establish what permissible data retention measures are. However, it must also be remembered that the EU does not currently have the competence to decide on blanket data retention measures for national security.

4.2. DRIPA: Substantive Issues including compatibility with CJEU decision

Panellists: Thomas Brennan (privacy policy advisor to Julian Huppert MP), Caspar Bowden (independent privacy advocate), Graham Smith (Bird & Bird)

The second session focused on analysing substantive issues of DRIPA; its compatibility with the CJEU data retention decision and the extraterritorial search powers granted to law enforcement in section 4 DRIPA.

Graham Smith observed that section 5 of DRIPA has amended the already very broad Regulations of Investigatory Powers Act 2000 (RIPA) definition of "telecommunication service" which is now even broader.[12]

In addition, section 4 of DRIPA amends Part 1 of RIPA to "enable warrants to be served on persons outside the UK, and may relate to conduct outside the UK".

---

[10] The European Parliament has since asked the Court of Justice for an opinion on the fundamental rights compatibility of the EU-Canada agreement on the transfer of Passenger Name Records before holding a final vote to approve it (2014/2966(RSP)).

[11] *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez* (2014), available online at: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

[12] A telecommunications service under s.2 RIPA was defined as "provision of access to, and of facilities for making use of, a telecommunications system". s.5 DRIPA has amended this definition to include any service that "consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system".

Serving UK notices and warrants in other countries is questionable from an international law point of view. However, Smith noted that DRIPA goes to great length to avoid violating international law by devising ways of serving warrants and notices within the UK on non-UK entities. There is a potential conflict of laws, which DRIPA has a mechanism to try and reconcile. But enforcing compliance with a warrant served overseas could be difficult, because there is a presumption that criminal offences do not apply to conduct and people outside of the UK.

Caspar Bowden focused on the way in which s.16 of RIPA relates to the extraterritoriality clause introduced by DRIPA. He explained that s.16 RIPA introduces a third warrant option for GCHQ beside the domestic interception warrant for use inside the UK, and the trawling warrant for external communications. This third option authorises GCHQ to scan all nominally external communications it captures to target a person known to be inside the UK. The speaker pointed out that this section was deliberately drafted to be difficult to understand and that few of the politicians who had voted for it at the time had truly comprehended its significance. He argued that section 4 of DRIPA complements this s.16 warrant in so far as it allows untargeted search of data outside the UK (for example, data available on Facebook).

4.3 Procedural and Constitutional Issues

Panellists: Speakers from the Article 29 Working Party and EU institutions

The third session focused on the procedural and constitutional issues of DRIPA with an emphasis on the current judicial review cases and a report from EU institutions.

The first speaker focused on judicial review possibilities and harmonisation between member states. He highlighted that if a national law is at stake and reviewed for compatibility with EU law, the benchmark for this judicial review is the same under EU law and the European Convention. In particular, the UK has no opt-out from the EU Charter of Fundamental Rights. He further observed that the CJEU in its data retention judgment made it clear that mere collection and storage of communications data already constitutes an interference with the rights enshrined in Article 7 and 8 of the Charter that needs to be justified. This means that the retention of the data needs to be strictly necessary. Data retention measures should therefore only be undertaken if absolutely indispensible. As a result of the judgment, the EU asks member states to remedy their national laws.

The speakers posed the question whether data retention at EU level will return. The Commissioner at the time rejected this, however, the new Commission under President Jean-Claude Juncker may of course decide otherwise.[13] However, the speaker pointed out that Juncker has promised to focus on data protection issues and the rule of law.

The speaker raised concern that national data protection regimes in place and amended in light of the CJEU judgment will differ. This is likely to reinstate a fractured approach across the EU as was the case before the Data Retention Directive harmonised national laws.

---

[13] Home Affairs Commissioner Dimitris Avramopoulos told the European Parliament's Civil Liberties Committee meeting on 3 December 2014 that the Commission is continuing to examine the options for data retention, guided by the Court's judgment.

As regards the question of extraterritorial conduct the speaker highlighted that there is political pressure within the European Parliament and Council to have general rules that prohibit access to extraterritorial data. Mutual legal assistance agreements are in place to facilitate access where this is necessary, and access requests should be made through these official channels. In the speaker's opinion, DRIPA is therefore a bad sign for other countries, who will use the UK as an example to introduce similar legislation. He observed, however, that issues of national security are not within the competence of the CJEU so that there is a limit to what EU institutions can do if member states adopt national laws to replace the invalid Directive.

Another speaker focused on the consequences of the judgment and DRIPA, which he saw as a necessary reference point when developing new data retention regimes.

He explained that because the CJEU did not go into detail on how retained data is accessed and used by law enforcement and security services during investigations, this would now make it more difficult to show that data retention measures were necessary as such. He argued that by introducing DRIPA the UK seemed to be dismissing the court's concerns as a mere nuisance.

As a result, the speaker found that clarity is needed on how the EU could approach law enforcement access to retained data. Retention should be targeted and proportionate, while at the same time giving police the necessary access. He argued that a dichotomy exists between electronic service providers and internet service providers, which the UK sidestepped by referring back to the RIPA definition of telecommunications operator. The speaker suggested that a code of practice at EU level should be developed to enable law makers to undertake a proportionality test before a law is proposed.

The final speaker reminded the audience that a pressing social need for a data retention regime at EU level exists. He reported that, for example, in Germany criminal prosecutions are still ongoing where communications data was the key evidence.

He argued that the CJEU mandated exceptions to retention requirements for professions with special confidentiality needs (for example, where communications are covered by legal privilege). These professions cannot be protected under general data retention regimes. However, the UK government's response to this issue in the context of the discussion surrounding DRIPA was to develop a database which, while initially retaining all communications data, would make it possible to filter out privileged information. Both the speaker and the audience were unconvinced that this would ensure compatibility of DRIPA with the principles set out in the CJEU decision.

The speaker concluded with a comment on the extraterritorial issue and argued that such provisions are either useless, or bring foreign telecommunication services in an impossible position. For example, Deutsche Telekom is not allowed under German law to disclose personal data to foreign law enforcement services outside formal international agreements. A unilateral power of UK law enforcement services to request this information would not relieve it from legal obligations that applied to it in its own jurisdiction.

4.4 Unconference Group Sessions

After lunch the workshop reconvened with less structured unconference group discussion sessions. Participants were divided into two groups: academics and civil society members. Other delegates were free to join either group.

The groups were asked to consider:

- What further research in the area of data retention and surveillance is necessary to inform the ongoing policy discussion?
- What type of expertise is needed to carry out this research?
- The next steps for judicial review and public debate.
- What need for collaboration with civil society and policymakers exists?

Suggestions for additional research made during the discussion include:

- What kind of analysis of retained data is helpful to investigations?
- Whether data retention has had any impact on crime rates?
- A comparison between crime rates in countries which do and do not have data retention law.
- Types of legal redress that could be suitable for those whose data is retained and/or accessed unlawfully?
- What categories of victims (and potentially suspects) should not have their data retained.
- What happens to retained data once it has been used? Could a trusted team look into random cases or samples to determine this?
- What data was essential for investigations of law enforcement and intelligent agencies?
- What crimes should not be investigated through data retention? For example: copyright, telephone harassment? To what extent is the use of retained data proportionate and can a slippery slope effect be avoided?
- Is there institutional overuse of retained and intercepted data? It was suggested that a study should be carried out to enhance available statistical data.
- How long will the current approach work, given for example, the ability to encrypt communications (horizon scan)?
- What is the material and territorial scope of fundamental rights protection inside and outside the EU?
- The extent to which criminal offenders are likely to adapt to investigative powers (e.g. burglars wear gloves to avoid DNA traces). Will measures taken by offenders make communications data useless?

It was suggested that further collaboration with industry could be fostered by interviewing companies to establish why they do or do not keep specific types of data and by studying relations between public and private actors in this area.

Suggested practical steps to address these issues include a need to:

- Identify time frames, potential funders and partners.
- Carry out research in the relevant time frames for policy making with quicker responses to achieve the highest impact.

- Collaborate on and coordinate consultation responses including peer-review of those responses.
- Collaborate with academics from other countries, potentially in the form of cross-EU partnerships.
- Establish a working network and funding sources for these types of activities.

5. Next Steps

After the group sessions, the participants reconvened and the respective chairs briefly updated the other group on the main points that evolved from the unconference sessions. Given this desire for further collaboration on the part of most of the participants, action points for near future cooperation and next steps were defined. They include:

- Setting up a "rapid response force" list of academics, who can quickly react to relevant policy developments and intervene in specific cases.
- Establish a forum where civil society groups talk to other interest groups about their needs.
- Publish academic analysis of DRIPA, where possible, in open access forums to guarantee public access[14]. Working papers might be better suited as a short-term solution.
- Set up a link farm for non-academics.
- Determine the issues politicians like to be briefed on.
- Put together a series of policy papers focusing on specific topics.
- Respond to other people's reports where appropriate.
- Establish better links with media and ensure good communication.

6. Conclusions

The workshop was very well received and most participants were eager to continue some form of collaboration. The summaries of the plenary talks and the unconference sessions show that much about this topic is still vague and requires clarification to establish legal certainty on the topic. This applies, in particular, to the extraterritorial powers introduced by DRIPA, with more than one participant commenting that this was a measure that was not well received in other EU countries and that could lead to retaliatory measures from other countries. Although the workshop could not deal with all the issues and questions raised by the participants it provided a solid basis for future steps designed to enable more in-depth analysis. It was also successful in establishing common ground and initiate collaboration among the different groups.

[14] For a first analysis following the workshop, see G Smith and J Rauhofer, "Mandatory communications data retention lives on in the UK - or does it?", Practical Law, 21 August 2014; available at http://uk.practicallaw.com/8-577-6488.