A critical analysis of Internet Connection Records in the Investigatory Powers Bill 2015

Supervisor: Peter Komisarczuk

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date: 15 August 2016
# BIBLIOGRAPHY

---

**THE DANISH EXPERIENCE** ................................................................. 55
INTRODUCTION ........................................................................................... 55
OVERVIEW ................................................................................................. 55
COMPARISON OF THE DANISH EXPERIENCE AND THE UK .................. 56
SUMMARY OF MAIN POINTS .................................................................... 58
CONCLUSIONS ......................................................................................... 59

**AVOIDING THE IMPACT OF ICRS** ....................................................... 60
INTRODUCTION .......................................................................................... 60
VIRTUAL PRIVATE NETWORKS (VPNs) ...................................................... 60
ENCRIPTION ............................................................................................... 61
TOR- THE ONION ROUTER ...................................................................... 62
WIRELESS MESH NETWORKS ................................................................. 63
PROTEST BROWSE ................................................................................. 64
SUMMARY OF MAN POINTS .................................................................... 64
CONCLUSIONS ......................................................................................... 65

**SUGGESTED FUTURE LINES OF RESEARCH** ........................................ 66
INTRODUCTION .......................................................................................... 66
IP ADDRESS RESOLUTION ...................................................................... 66
UTILITY OF ICRS ..................................................................................... 67
AVOIDANCE METHODS ........................................................................... 67
DEFINITIONS ............................................................................................ 68
ACCOUNTABILITY AND OVERSIGHT ...................................................... 68
CONCLUSIONS ......................................................................................... 68

**CONCLUSIONS** .................................................................................. 69
THE CONTEXT TO THE BILL ................................................................... 69
DEFINITION .............................................................................................. 69
HOW AN ICR WORKS ............................................................................ 69
PURPOSE OF ICRS .................................................................................. 70
DANISH EXPERIENCE ............................................................................ 71
AVOIDING THE IMPACT OF ICRS ......................................................... 71
FINAL CONCLUDING REMARKS ......................................................... 72
VALUE OF THIS RESEARCH ................................................................. 73

---

---
List of Figures and Tables

Figure 1: showing how ICRs could be used to identify a device in a real case, p 20

Figure 2: Breakdown of 100,000 Communications Data Applications submitted under section 22(2)(b) RIPA by Crime Type, p 41

Figure 3: Most prevalent accessed applications on 27 seized mobile phones, p 42

Figure 4: showing how identifying a device could be useful in law enforcement investigation, p 43

Figure 5: Example of Communications Data held by CSPs for internet based communications, p 44

Figure 6: Example of what an Internet Connection Record could look like, p 44

Figure 7: showing how an ICR could be used to identify a service used, p 46

Figure 8: communications data from obtained from firewall, p 51
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT</td>
<td>British Telecom</td>
</tr>
<tr>
<td>CDN</td>
<td>Content Delivery Network</td>
</tr>
<tr>
<td>DRIPA</td>
<td>Data Retention and Investigatory Powers Act 2014</td>
</tr>
<tr>
<td>GCHQ</td>
<td>Government Communications Headquarters</td>
</tr>
<tr>
<td>ICRs</td>
<td>Internet Connection Records</td>
</tr>
<tr>
<td>IOCCO</td>
<td>Interception of Communication Commissioner's Office</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPB</td>
<td>Investigatory Powers Bill</td>
</tr>
<tr>
<td>ISPs</td>
<td>Internet Service Providers</td>
</tr>
<tr>
<td>MI5</td>
<td>Security Service</td>
</tr>
<tr>
<td>MOSH</td>
<td>Mobile Shell</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NCA</td>
<td>National Crime Agency</td>
</tr>
<tr>
<td>NGO</td>
<td>Non Governmental Organisation</td>
</tr>
<tr>
<td>OFCOM</td>
<td>Office for Communications</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PLR</td>
<td>Preliminary Literature Review</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SIS</td>
<td>Secret Intelligence Service</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>VPNs</td>
<td>Virtual Private Networks</td>
</tr>
</tbody>
</table>
Abstract

The chapter ‘Context to the Legislation’ aims to give the reader an overview of the why the Government felt that the legislation was needed. This chapter also covers the current legislation around communication data and the difference to this ICRs Investigatory Powers Bill would make. The chapter ‘How an ICR works’ deals with the actual mechanics of who can apply for communication data, the obligations on the ISPs to provide that data and the observation that ICRs may well differ between ISPs. The chapter ‘The Purposes of ICRs’ explores what functions ICRs hope to fulfil, and the way that communication data could be used in investigations. The chapter ‘Danish Experience’ aims to give the reader a comparison with an attempted scheme that was aborted in Denmark. Comparisons and differences with the proposed UK are analysed to see if lessons can be learnt from the Danish experience.

The chapter ‘Avoiding the Impact of ICRs’ explains to the reader how the aim of ICRs can be avoided. This includes by the use of VPNs, anonymising tools and the use of alternative technologies. The chapter ‘Further Research’ aims to highlight other research lines that have either been raised by this research or should be research lines in their own right.
Executive Summary

This research has looked at one of the central tenants of the Investigative Powers Bill; that of Internet Connection Records. It has attempted to define exactly what a ICR is. It is clear what kind of communication data is likely to be in an ICR but the legislation has avoided giving a categorical definition of what an ICR is. This is in keeping in the spirit of Parliamentary legislation, where definitions are usually broad and more detailed in secondary instruments. It is also a deliberate attempt to ensure that the legislation does not have to be revisited by allowing those communication data types collected to change. This is an inherent tension in the Bill between those who want clear and precise definitions, and those who prefer a more flexible approach.

Although the Bill outlines four purposes for ICRs, they can be condensed into two main areas; identifying devices and identifying internet services used. The purpose of this is to give investigative leads to law enforcement. The number of applications for communications data under existing legislation is increasing, and is already at high levels. The vast majority of these applications are not for serious crimes. ICRs are intended very much to be a tool of law enforcement and the intelligence services already have significant capability in this area. Whilst the large number of applications for communication data at present would suggest its utility, there is no empirical evidence to conclusively say exactly what its impact has been.

One of the most important areas to come out of this research, is that the argument that ICRs will restore lost capabilities to law enforcement is misleading. All the powers contained in ICRs already exist in legislation. What the Investigatory Powers Bill will do is bring all those powers together in one place. Although it should be noted that the Bill does bring in new oversight arrangements.

This research has shown that while identifying devices and identifying services accessed on the internet is possible via ICR, they are not without challenges and they can potentially be easily avoided. This research has looked at session logging in Denmark
and highlighted the problems encountered there, whilst that the UK model has technical differences.

The ease with which individuals can bypass ICRs has been identified. These are all ‘easy’ solutions and it merely remains to be seen whether the introduction of the Bill will increase their use. This will require future research post the Bill becoming law.
Motivation

The draft Investigatory Powers Bill is currently before Parliament, having being scrutinised by three separate Parliamentary Committees [7,11,16]. The Bill has far reaching consequences and it is a controversial piece of legislation, given that at its core is the relationship between the government and its citizens. The intention of the Government is that the Bill will be enacted in late 2016. The Bill has a number of aims: it brings together a lot of disparate legislation concerning interception of communications into one statute; it acknowledges a number of capabilities that have existed but have never been directly the subject of legislation; it brings in a new system of oversight for the use of those most intrusive powers. As such, the Bill’s scope is very broad, and will no doubt will be a source of much academic study and research for some time.

A new concept the Bill introduces is Internet Connection Records (ICRs). This was a new term that had not existed in the industry or in previous legislation. ICRs were going to be central to the new Bill, so the area of what an ICR actually was and what its impact would be, suggested a productive search project. Central to the initial review of ICRs was the realisation that there was not a clear definition to their scope. This element of what constitutes an ICR seemed an important question to determine, especially given ICRs prominent position in the proposed legislation.

The Preliminary Literature Review (PLR) of the ICRs looked at the technological impact, the legal impact and the consequences for the Internet Service Providers (ISPs). This review then narrowed down these research areas into the aims outlined. The research has endeavoured to focus on areas where productive research was possible. Some potential lines of research were not possible because they related directly to law enforcement operational capability, and others because of equipment manufacturers or ISP concerns of their own secrecy of particular technology.

The Bill, by virtue of being a draft piece of legislation, is still subject to scrutiny and change. Indeed, following the reports of the two scrutinising Parliamentary
Committees, there were a number of changes and revisions to the Bill. This process is likely to continue as the Bill proceeds to the statute book. This research has endeavoured to keep the work presented current of the latest developments. Any omissions in this changing area of draft legislation are the authors alone.
Aims and Objectives

a  Determine the concept of an ICR in the context of the Bill, law enforcement and digital communications community.

b  Investigate whether ICRs are an effective measure against criminality in the way it is proposed.

c  Determine if there are ways ICRs can be avoided.

d  Investigate any comparisons with systems that have been attempted in other countries.

These are the main aims and objectives that will be concentrated on in the course of the research. The outputs of my project will be:

1. To place the Investigative Powers Bill, and ICRs in that Bill, into context i.e. what has made the Government want to introduce this legislation.

2. To provide clarity as to what communications data is in an ICR, and if that is not possible, to explain the reasons why.

3. To explain the purpose of ICRs and if they are needed.

4. To make a comparison of other countries use of similar systems

5. To highlight the ways ICRs can be avoided and to assess if these undermine the effectiveness of ICRs.
Main Research Documentation

Parliamentary Committees

After the Bill was proposed, there were three Parliamentary Committees that scrutinised and reviewed the legislation [7,11,16]. The first of these was the House of Commons Science and Technology Committee Investigatory Powers Bill: technology issues [16]. As the title suggests, this was a report looking into the technological implications of the Bill, and not the wider implications of the Bill on society:

*In our inquiry we have focused on critical technological aspects of the draft Bill. We have not addressed the need or otherwise for the communications monitoring provisions or whether they are proportionate to the threats they are intended to deal with. Our focus has been on how the main technological issues involved might affect the communications businesses that will have to collect data and provide access to the security authorities.*

The Committee received over 50 written submissions and held two separate oral evidence hearings. The issues surrounding the use of internet connection records were central to the report, and one of the the four final chapters of the report was solely related to ICRs. Their report was published on the 1st February 2016.

The second of the Parliamentary Committees was a combined Committee on the House of Lords and the House of Commons [7]. This had a far wider remit and scrutinised the Bill as a whole. This broader remit can be seen from the number of submissions it received from interested parties, numbering some 148 written submissions. The Committee also heard extensive oral evidence too. The purpose of this pre-legislative scrutiny was:

*The Committee has sought to give the greatest possible early opportunity for stakeholders and the wider public to comment on the draft Bill. In legislation of particular controversy, where many of the facts underpinning arguments on*
Although the technology issues had been covered by the Science and Technology Committee, the Joint Committee considered these aspects as well. It also paid considerable attention to the issue of ICRs. The Committee published its report on the 11 February 2016.

Whilst these two reports were the starting point for the research undertaken, they concentrated on the Bill in its totality and not just specifically ICRs. The main bulk of the research relating to this project was the oral and written evidence to these two committees.

There was a third Parliamentary scrutinising committee into the Bill which was by the House of Commons, Intelligence and Security Committee [11]. This Committee was looking at how the Bill would effect the intelligence services; the Security Service (MI5), the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ). This Committee made only the briefest of comments on ICRs and its inclusion here is mentioned for completeness.

Surrounding Documentation

There were a number of important documents that were released, by the Government or the Home Office, which were directly related to the Bill. There were a number of factsheets issued alongside the Bill, including one on ICRs [17]. The Home Office released an important source document on the operations reasons for ICRs [13]. This explained the operational reasons ICRs were required by law enforcement.

Some of the most important documentation surrounding ICRs was released by the Government following the publications of the above Parliamentary reports. The Government accepted the majority of the recommendations made by the reports in its written response [14]. One of the specific recommendations of the Joint Committee was
the Home Office should look at the Danish experience of session logging which they had heard written and oral evidence on. The Government did conduct a comparative investigation and released a report on this [15].
Context to the legislation

Introduction

ICRs are a construct of the Investigative Powers Bill. Therefore, to fully understand them, we need to have an overview of current legislation in relation to interception of communication data. This chapter will consider: - the technology changes that have changed the way we communicate; the current legislation that governs access to this data; and the specific capability gaps that, law enforcement argue, is needed for the introduction of ICRs.

Technology Changes

“The means available to criminals, terrorists and hostile foreign states to co-ordinate, inspire and to execute their plans are evolving. Communications technologies that cross communications platforms and international borders increasingly allow those who would do us harm the opportunity to evade detection.”[66]

Communications patterns and the technologies that underpin them are changing. Furthermore, the rate of that change has been very rapid. The most important shifts are the rise of the smartphones and the increasing access of online services, especially communication services. According to Office of Communications (OFCOM) the smartphone has now overtaken the laptop as the most common way to access the internet [6]. Its use amongst the young, is ubiquitous. What is striking is how much communication is now done over the internet, from emails to instant messaging, with emailing being the most prolific communication used [6].
Current Legislation

The main piece of legalisation surrounding access to communication data is the Regulatory Investigatory Powers Act 2000 (RIPA) [2]. This Act deals with the acquisition and disclosure of data but critically does not deal with the retention of data i.e. ISPs are under no obligation to retain communication data. Following the terrorist attacks on the US in September 2001, a voluntary code was adopted. This code required that details of websites visited, by a UK customer, were retained [9]. Subsequently, a European Union Directive [3] made this requirement mandatory.

The Government felt this legislation was not completely adequate, and published in June 2010, the Draft Communications Data Bill [4]. This draft Bill was heavily criticised, both in the media (where it was dubbed the ‘snoopers charter’) and during the legislative scrutiny process, where its provisions were seen as too onerous. This Bill was not progressed beyond the draft stage. A contributory factor in this, was that the coalition government disagreed between themselves about the provisions and breadth of the Bill.

In 2014 the European Court of Justice declared the EU Data Protection Directive invalid on privacy grounds [5]. Following this ruling, the Government enacted the The Data Retention and Investigatory Powers Act 2014 (DRIPA) [8] to allow for the continuing retention of communications data. This Act was designed to be a temporary piece of legislation as it was specifically written to expire at the end of 2016. At this stage, it was clearly felt by government, that there was a need for a single Act to bring together all the legislation. Therefore, the the draft Investigatory Powers Bill was introduced.

Stated aims of the Bill

The Bill had three main aims, highlighted below:
• First, it will bring together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will make these powers – and the safeguards that apply to them – clear and understandable.

• Second, the draft Bill will radically overhaul the way these powers are authorised and overseen. It will introduce a ‘double-lock’ for interception warrants, so that, following Secretary of State authorisation, these – and other warrants – cannot come into force until they have been approved by a judge. And it will create a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.

• Third, it will make sure powers are fit for the digital age. The draft Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate. [1]

The reference to the third aim shows how central the ICRs are to the Bill. The draft Bill was published in November 2015, along with some supporting factsheets on aspects of the Bill [17]. There were three separate Parliamentary Reports on the Bill [7,11,16] which all reported in the Spring of 2016. Following this, the Government responded to these reports recommendations [14] and the Home Office released a number of documents [12,13,15] clarifying areas of the legislation.

Capability Gaps that ICRs seek to address

The Bill itself, the surrounding supporting documentation, and the majority of the evidence given to the two committees [7,16] makes clear that ICRs are essential, in restoring capabilities that have been lost as a result of the changes in the way people communicate. In the course of this research, it has been difficult to fully ascertain what those lost capability gaps are. These argued for capability gaps are considered below.
One of the capability gaps relates to the retention of data. The Bill will legally obligate ISPs to retain data, for up to 12 months. There is no specific data retention requirement in RIPA, which deals with the circumstances in which data can be accessed. The 12-month retention period is important as it allows investigators to look at historical communication data and not just immediate communication data. This is seen as important, especially in child exploitation and tax cases. ISPs would only normally hold data that is relevant to their business purposes.

In the first instance, it would seem that the 12-month retention period is an increase in law enforcement capability. However, DRIPA allows the Home Secretary to issue notices to retain data, and importantly for a 12-month period. So the capability that law enforcement argues that has been lost, already exists. There are two important provisos to this. Firstly, the DRIPA was brought in as a piece of emergency legislation following the European Court of Justice decision in Digital Rights Ireland [5]. DRIPA specifically states, that the Act will be repealed on the 31 Dec 2016. Thus, new legislation will be needed. Secondly, the definition of ICRs presented in the Investigatory Powers Bill is such that it can be changed depending upon changing circumstances (see ICRs definitions). However, the power to retain communication data already exists, in this instance, so ICRs are not restoring a lost capability.

During oral evidence at the Joint Committee [7] there was much discussion as to the need for the 12-month retention and whether a shorter period of time be sufficient. As the Director for National Security, Paul Lincoln, at the Home Office noted in his oral evidence:

*The critical reason for going up to 12 months is child sexual exploitation cases. Certainly when a survey was done on this in 2012, 49% of all requests made in child sexual exploitation cases were for data between 10 and 12 months old. That is a very significant period, which is reflected in the position that we have taken.* [67]
Similar arguments were made by the Her Majesty’s Revenue and Customs (HMRC) in relation to tax cases. However, Paul Lincoln, acknowledged in the the same oral evidence that the 12-month period was not new:

*It is also worth clarifying that the period for a maximum of 12 months for communications data is already current practice in terms of data being stored by those that are under a data retention notice. So that is not a new proposal. [67]*

This I believe is referring to the provisions in s 1 (5) DRIPA, although this is not explicitly stated. Thus the retention period of 12 months is neither a new proposal, or a lost capability gap. However, even the Home Office’s own documentation, released shortly after the draft Bill, makes clear the key capability of ICRs is the retention of data:

*The Bill will enable us to require providers to collect and retain internet connection records, allowing law enforcement agencies to attribute illegal activity on the internet to a person in the real world. [17]*

It is unclear why this power is being presented as a lost capability when it is not.

Another area where current legislation is deemed to be leading to a capability gap, is the issue of IP address resolution, which is a primary stated aim of ICRs. Figure 1, below shows how law enforcement could would benefit from using ICRs. In this real case ICRs were not available.
However, s 21 Counter-Terrorism and Security Act 2015 deals specifically with IP address resolution, in language very similar to ICRs. Therefore, again this is not specifically a new power. So the case in Figure 1 could now be investigated without the provisions of ICRs in the IPB.
The National Crime Agency in a written submission to the Joint Committee appeared to acknowledge that the Bill presented them with no new capabilities:

*All powers available to law enforcement under the IPB are currently available under existing legislation. The only exception to this is in relation Internet Connection Records (ICRs), where it is proposed that a new obligation should be placed on service providers to maintain records of ICRs.* [68]

Again, it is worth disputing the point on retention of record as this already exists in DRIPA.

Reading extensively through the oral and written evidence to both committees and surrounding documentation, there was no clear evidence of what the problems were with existing legislation. What powers that were mentioned, already existed, albeit in different Acts. It seems, therefore, disingenuous to suggest that ICRs bring in new capabilities or lost capabilities that are not already in existence. What can be said is that those capabilities are being brought together in one single piece of legislation, rather than being found in several pieces of legislation. This will no doubt add clarity and transparency but the argument that these powers are restoring lost capabilities is not valid.

**Summary of main points**

- There has been a significant change in the way we communicate, with smart phones and Internet serviced communication becoming the dominant way of communicating.

- It is always a huge challenge for legislation to keep pace with rapid technological changes.

- The main piece of legislation in this area is RIPA, although there are others.
• The Investigatory Powers Bill aims to bring together all the legislation in the area into one Act. It further proposes new ways these powers are authorised and overseen. Finally, the Bill brings in the concept of ICRs.

• Although the Bill makes clear that ICRs will restore capabilities that have been lost. There seems little clear evidence for the validity of this statement. The author’s own analysis suggests that these powers are already there in current legislation.

Conclusions

The Bill recognises that the majority of people are communicating in different ways. Whether legislation is able to keep pace with this will be considered in latter chapters. The Bill's aims in consolidating legislation into one Act is sensible, but some of the rationale for this i.e. regaining lost powers, does not stand up to scrutiny on analysis. This is probably more reflective on the sheer vastness and complexity of the criminal law than a deliberate attempt to deceive. However, the claims made do no stand up to rigorous analysis.
How an ICR works

Introduction

This chapter is about how, from an examination of the Bill, an ICR actually works in practice i.e. how is a request made, on what grounds and how is the request dealt with by the communications provider (in most cases the ISP). There is a new, planned system of oversight governing all this, but this will not be covered by this research.

The concept of ICRs is being introduced very much from a law enforcement perspective and this will be explored below. This is an important point as many of the other provisions of the Bill deals with capabilities of the intelligence services (SIS, MI5 and GCHQ).

There are a number of obligations placed on ISPs when they receive a data retention notice and these will be outlined.

Law enforcement v Intelligence Agencies

It is an important point to make is that the ICRs are primarily concerned with law enforcement and not the intelligence services. This point was made clear by the Intelligence and Security Committee on their report on the Investigatory Powers Bill:

*The draft Bill also introduces a new power for law enforcement organisations and the Agencies to acquire Internet Connection Records (ICRs). The Agencies have told the Committee that, given that they have a range of other capabilities which enable them to obtain equivalent data (and the fact that they do not have the same requirements for evidential material as law enforcement), the power to obtain ICRs set out in Part 3 of the draft Bill will be used primarily by law enforcement organisations. The draft Bill is not clear on this issue, resulting in a lack of transparency. [18]*
This was certainly reflected in the oral and written evidence given to the other Parliamentary committees, which in relation to ICRs was overwhelmingly concerned with law enforcement issues.

The important point here is that as ICRs will be used by law enforcement. Thus, there use should be clearly outlined definable limits as to what communications data can be used.

Confusion

There are problems in analysing the Bill as there is the difference in s 47 and s 71 (see also definitions). The former refers to ICRs whilst the latter refers to communications data. This confusion was accepted by the Government [14] in their response to parliamentary scrutiny:

and a single definition of ICR has been created, ensuring consistency across parts 3 and 4 of the Bill which provide for acquisition and retention respectively [25].

These two different concepts shall be dealt with in turn.

Who can make an ICR Request - Acquisition

The ability of who can make ICR requests was limited to police forces and the National Crime Agency (NCA) [19]. Although a certain number of public authorities i.e. HMRC can also make applications in certain circumstances [20], this is a limitation from the original Draft Communications Bill of 2010, which included local authorities. This came in for much criticism, particularly as a result of how some local authorities had used RIPA legislation for very minor offences [21]. However, the latest version of the Bill does now allow for local authority use of ICRs. However, this is under a different set of access criteria and will not be further considered here.

The power to grant an authorisation is made by a ‘designated senior officer’ from the police or public authority. This, would not normally be an officer who is working on
that case [22], except in exceptional circumstances [23]. The range of circumstances an ICR can be authorised, is detailed in the Bill [24] but these must be ‘necessary and proportionate’.

Powers to require retention of data - Retention

Only the Home Secretary by notice is able to issue a notice to require a telecommunications operator to retain data for up to 12 months [26]. The test is whether this is ‘necessary and proportionate’.

In many ways this is the most controversial area of the Bill. As discussed in ‘definitions of ICRs’ the Bill gives a very broad definition of ‘communications data’. Defenders of this, argue that this gives some future proofing, whilst others argue it gives too broad and sweeping powers.

It is important to note that no action is required by ISPs until a notice is served. This was reiterated by the Government in their response to the Parliamentary Committee scrutiny [34]:

*There are a number of factors which the must be taken into account before issuing a retention notice. These include; the likely benefit, the likely number of users of the telecommunications service, technical feasibility and the cost of complying with the notice [27].*

The Home Office must take steps to consult with the operator before the notice is issued [28]. This is seen as allowing both the telecommunications provider and the Home Office to see what is realistically possible. Evidence from the Home Office [29] to the Joint Committee demonstrated that they had had significant contact with the larger ISPs on this issue. The Home Office did not envisage serving notice on all the 200-300 ISPs, perhaps recognising that the cost and feasibility of some of the smaller operators may make this not worth while. Alternatively, this could be a factor of the UK
architecture, that means most communication passes through the larger ISPs at some point.

Obligations on ISPs

The telecommunications provider is under an obligation to ensure the security of the data they collect [30]. There was some discussion in both of the committees by various parties, giving evidence that this was a potential weak point in the system. In many ways the Government is avoiding the responsibility for the storage of this data and placing that responsibility on the ISPs. This area will certainly warrant further research.

In the original version of the Bill, the ISP was not to disclose the existence of a notice [31]. Many ISPs had criticised this, in that they wanted to be able to discuss how to implement an ICR with other ISPs, particularly in respect of technological areas. However, in the Home Offices’ draft code of practice, following the recommendations of the two Parliamentary Committees, ISPs will now be allowed to discuss the notice with the approval of the Home Office [32].

The telecommunications operator may refer the notice back to the Home Office as to the technical requirements or the financial consequences [33]. This in effect reflects an appeal mechanism.

Summary of main points

• ICRs are mainly concerned with law enforcement (with some limited access now for local authorities)

• Power to grant authorisation is limited to a ‘senior officer’, who in normal circumstances is not connected to the investigation.

• Only the Home Secretary can authorise retention of data, who must take account of a number of factors such as necessity and proportionality in their decision.
• ISPs do not need do anything until they are served a notice.

• The Home Office must consult with a telecommunications operator before an ISP is issued.

Conclusions

The Bill sets out how the ICRs will work. One of the major problems, as discussed in definitions of ICRs, is that ICR as a term is only mentioned explicitly in the Bill once. This means that the Bill can make for difficult reading and analysis. The Bill has been amplified by a more recent draft code of practise, issued by the Home Office. The major points to be highlighted from this research perspective is that what constitutes an ICR still remains unclear. This is for reasons of future-proofing the legislation.
Definition of Internet Connection Records

Introduction

The accurate definition of what an ICR is, and what data an ICR consists of, is a primary research aim of this thesis. The lack of a clear definition in the Bill as to what an ICR is, coupled with the fact that the term is not a recognisable one by industry, has caused much confusion and debate. Given that the term is so central to the Investigatory Powers Bill, it is of great interest that there is sufficient clarity to this term.

The use of the term ICR, as statutory language in the Bill, will be investigated. Further to this, official supporting documents released by the Government, will be analysed to see if this can bring further clarity to the term. The comments of, and evidence presented to, both the Joint Committee and the Science and Technology Committee [7,16] will be considered, particularly with respect to the demands placed on ISPs – who ultimately will collect and retain ICRs. In so far as we are able to, an attempt will be made to ascertain what data is contained in an ICR, and the issues that surround that definition. It is only by coming to the clear idea of what an ICR is, are we able to fully understand the impact ICRs will have.

ICR’s defined in the Bill

Given the importance of the term to the Bill, it is surprising in that there is only one direct reference in the Bill to ICRs:

In this section “internet connection record” means data which—

(a) may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and
(b) is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person) [35]

This is a very broad and vague description. Any telecommunications provider reading this definition would legitimately ask ‘but… what data do you want me to provide?’ Such a broad definition is not likely to be Parliamentary draughtsmen’s error but a conscious decision to ensure that the Bill is flexible enough to adjust to changes in technology, and the patterns of how we communicate. The Danish experience, which is discussed later on, suffered from the explicit problem of not only a prescriptive definition but also by not envisaging the growth in shared IP addresses, which had huge implications on the utility of data collected.

The counter argument to this is that the ISPs are unclear, from the Bill, what data they will need to provide. Given that these are the bodies that will have to implement the legislation, the onus is on the Government to provide clear and unambiguous legislation as to what those commitments are. This is not possible, or more accurately is unclear from this definition. Critics of this viewpoint may argue that the legislation can be ‘fleshed out’ through the use of statutory instruments, or developed through case law relating to the Act. However, given the controversial nature of the legislation, with its implications on civil liberties, it should be a clear and precise definition. This is important as it is the Bill that is subject to Parliamentary scrutiny, not latter statutory instruments such as secondary legislation or codes of practise.

The passage of the Bill outlined above is the only direct reference to ICR in the whole Bill. A far broader definition is expanded upon later in the Bill but this does not specifically mention ICRs. Whilst it would appear that the part of the Bill is referring to ICRs, this is not explicit. Instead the Bill refers to ‘communications data’:

The Secretary of State may by notice (a “retention notice”) require a telecommunications operator to retain relevant communications data if the
Secretary of State considers that the requirement is necessary and proportionate… [36]

It is unclear why this is not referred to as an ICR, as it would offer greater clarity in the Bill. It was a specific recommendation of the Joint Committee that the definition of ICRs should be consistent throughout the Bill [37]. However, ‘communication data’ is later defined in the Bill as:

In this Part “relevant communications data” means communications data which may be used to identify, or assist in identifying, any of the following—

(a) the sender or recipient of a communication (whether or not a person),
(b) the time or duration of a communication,
(c) the type, method or pattern, or fact, of communication,
(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted,
(e) the location of any such system, or
(f) the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program. [38]

This is a ‘tighter’ definition than the proceeding one, albeit still with considerable scope. It is clear that the IP address, the unique identifier of a piece of communication equipment on the Internet, is one of the main pieces of data required. Critics of the Bill will argue that this more expansive definition is still not sufficiently definitive.

This is a tension that will be a common theme throughout – the difficulty of defining an ICR that will keep pace with a rapidly changing environment, versus the need to have a clear outline of the limits of the government’s powers. Indeed, this ‘tension’ or ‘friction’ between these two paradigms can be clearly seen in the evidence of the Home Secretary, to the two main Parliamentary committees on the the Bill. On referring to ICRs, she acknowledged the need for them to be:
… that we are trying to draft legislation that will operate in what can be quite a fast-moving technological world, where things are developing. The more you try and prescribe in more and more specific definitions, the harder it becomes and the shorter the life of the legislation is likely to be. [39]

What is clear is that there is a desire for Parliament to not have to continually reintroduce or update legislation, every time current capabilities are overtaken by changes. This can be seen from the Danish example, discussed more fully later, where they failed to predict the growth in IP addresses. This led to the use of IP address sharing which rendered much of the data collected under a broadly similar scheme, ineffective.

It is this issue as to whether the definitions are so broad that will be the subject of much debate. It is clear that the Parliamentary committees who scrutinised the Bill had concerns in this area.

**Parliamentary Scrutiny**

The two main scrutinising committees, namely the Joint Committee and the Science and Technology Committee, both expressed concerns over ICRs. In its summary the Joint Committee concluded that ICRs:

….. *But we also heard strong concerns, in particular from some of the providers themselves, about the lack of clarity over what form the ICRs would take….*[40]

It made a specific recommendation (recommendation 12) about the definition of the term and welcomed further guidance on this matter, from the Home Office.

Similarly, the Science and technology Committee in its conclusions, noted that:

*The Government, in seeking to future-proof the proposed legislation, has produced definitions of internet connection records and other terms which*
have led to significant confusion on the part of communications service providers and others. [41]

These recommendations and conclusions, reflect the wide ranging evidence to the committees on the lack of clarity to ICRs. Some of this discussion is to be expected as the term is not one that the industry is familiar with. Indeed, the term ICR is one that has been specifically constructed for the Bill. So whilst some of the criticisms over lack of clarity may be valid, it must also be recognised that any new concept or terminology, particularly in the controversial area of civil liberties, will always attract much discussion. The Government appeared to recognise this fact, and responded to the concerns and the Parliamentary scrutiny, by issuing further and more descriptive guidance on ICRs.

Further Guidance

Specifically, in response to these concerns the Home Office published a draft code of practice [14]. In this document an ICR is further defined as:

An Internet Connection Record (‘ICR’) is a record of an event held by a telecommunications operator about the service to which a customer has connected to on the internet. An ICR is communications data which may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunications system for the purpose of obtaining access to, or running, a computer file or program. It comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication. In most cases ICRs will be held by internet access providers which are telecommunications operators which provide access to the internet and can include a home broadband connection, mobile internet or publicly available Wi-Fi. [42]
If this definition is compared to the definition of an ICR, in part 4 s 47 of the Bill, there is little new information, aside from further guidance on what a telecommunications operator may be. However, the document does add clarity on what that communication data may comprise of:

- A customer account reference – this may be an account number or an identifier of the customer’s device or internet connection;

- The date/time of the start and end of the event or its duration;

- The source IP address and port;

- The destination IP address and port – this is the address of the service accessed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc.);

- The volume of data transferred in either, or both directions;

- The name of the internet service or server connected to; and

- Those elements of a URL which constitute communications data – this is the web address which is the text you type in the address bar in an internet browser. In most cases this will simply be the domain name – e.g. socialmedia.com. [43]

The first point to note is that this is data that may constitute an ICR, and not data that will constitute an ICR – leaving the definition open to further change. Thus, this further guidance is only guidance and not prescriptive. It is however, more expansive than the definition of ‘communications data’ in the Bill. This is the first mention of; a specific account reference, the volume of data and the name of the internet service it is
connected to. Furthermore, there is an explicit reference to what elements of the URL constitutes communications data. This is important. There were many public statements, preceding and following the Bill, that the Bill was only concerned with what sites individuals looked at but not what content was looked at. However, this is never made explicitly clear in the Bill itself. Whilst there are other documents that outline this position, such as the ‘Operational Case for Internet Connection Records’, and the draft code practise itself, this is the first specific mention of what data would and would not be included.

Clarification of Communication Data

The Government accepted the majority of the recommendations following Parliamentary scrutiny, and its response to the issue of lack of clarity between communication data and ICR was that:

A single definition of an ICR has been created, ensuring consistency across parts 3 and 4 of the Bill, which provide for the acquisition and retention of communications data respectively [44]

The new definition for ICR is:

In this Act “internet connection record” means communications data which—

(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person) [45].
Note that this definition (as at 01 August 2016) is virtually the same as the original draft. Similarly, the new definition of ‘communications data’ is:

In this Part “relevant communications data” means communications data which may be used to identify, or assist in identifying, any of the following—
(a) the sender or recipient of a communication (whether or not a person),
(b) the time or duration of a communication,
(c) the type, method or pattern, or fact, of communication,
(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or
(e) the location of any such system, and this expression therefore includes, in particular, internet connection records. [46]

Which is again very similar to the original draft, with the exception of the explicit reference to ICRs. In conclusion, the amendments to the Bill do not significantly differ from the original draft versions.

The definition in the draft code of practise has given commentators, and the wider public, something more definitive to unpick and discuss. It is also worth noting here that the retention notice to be given to a communications provider, will not necessarily be the same. The principle behind the legislation enables the Home Office to frame the notion of what data is to be collected, according to the differing technical capabilities of the communications provider. This allows greater flexibility, given the disparate nature of ISP architecture in the UK.

The Government has chosen to give a broad definition in the Bill of what an ICR is. It has responded to the lack of clarity in that definition with giving, in effect, an example of what an ICR could look like. The reason for this lack of descriptive definition is that the Government wishes to future-proof the legislation i.e. to have not to continually update the legislation. It is normal for Parliamentary Acts of legislation that broad definitions are expressed in the main Act, and more substantive definitions are included in later legislative instruments. The fact that the Bill deals with such a sensitive area,
could be an argument for clearer definitions in the Act itself. That said, the definitions issued in the draft code of practise [12] are substantive enough to give clarity as to what could constitutes an ICR.

It is worth considering what alternative action the Government could have taken. A more explicit definition would most likely be overtaken by the rapid changes in the communications environment. This leads to the alternative option where the legislation is revisited every few years to keep the legislation abreast of changes. The Government has made a conscious decision that the legislation should as far as possible avoid this scenario, and has therefore given a broader and more flexible definition to an ICR.

Summary of main points

• There is a lack of clarity in the definition of ICR in the Bill, although this is within the Parliamentary tradition of legislation.

• There is inconsistency in the language of the Bill particularly between ‘internet connection records’ and ‘communications data’. This has been amended in the latest version of the Bill (as at 01 Aug 16).

• There was concern about the definition of the ICRs during the Parliamentary scrutinising committees.

• Efforts have been made by the Government, to provide greater clarity on what may constitute an ICR. Although there is an acceptance that the Bill is designed not to be continually revisited (future-proofing), which precludes a more descriptive definition.

• To have a more descriptive definition of an ICR would probably necessitate the legislation being regularly updated. This was not the intention of the Government.
Conclusion

One of the research aims of this project was to investigate what, and by definition define (what) an ICR was. This has been more difficult than what many would have expected. Science and technology is about certainty and precision. This view coupled with the commercial outlook of most ISPs means that they want a precise definition of what an ICR is, or more specifically, what data constitutes an ICR. However, from the lens of legislation, precise and definitive definitions can be problematic. A prescription definition would need to cover all eventualities, and can be difficult to keep pace with changing circumstances. Therefore, the tradition of UK legislation has been to keep definitions broad and add detail of implementation through statutory implementation.

In this instance, the situation is more problematic in that the Bill is dealing with the controversial area of civil liberties. Furthermore, the concept of ICRs is a new one, and one not yet fully understood by industry or the wider public. The definitions provided in the Bill, and expanded upon by subsequent documentation, are probably the best basis on which to base our understanding of ICRs on. Given that the communications data requirements are going to be different, depending upon the notice served on the ISP, then every ICR may have different requirements. Since the notices will be secret, it will be difficult to know, in the public domain, what a typical ICR is.

In this scenario, ICR may then not be seen as something with a clear definition, as many have argued, but rather a model. A model can be adapted to the particular circumstances and changing environment but its main principles remain the same. From this perspective, an ICR is merely a collection of data that allows a device to be identified and what services an individual is using. In this model there is a limitation in limiting the the data to the identification of those services but not the content. The utility and the difficulty in obtaining such data will be discussed in later chapters.
Purpose of ICRs

Introduction

This chapter is about the need for ICRs and why they need to be introduced. Individuals are communicating in different ways, away from traditional telephony methods to utilising the Internet. ICRs endeavour to adapt to this change. The Home Office has set out its vision of why ICRs are needed [13] and those aims will be critically analysed and assessed. This is important to make sure there is a congruent and persuasive argument for the introduction of ICRs. Furthermore, it is necessary to look at whether the aims set out for ICRs can be achieved.

Background

There has been a change in the way people communicate. Landline telephony gave way to the mobile phone and then the smart phone, often utilising the Internet in providing communications. The factual evidence that people are communicating in different ways can be seen in the following data provided of Ofcom, and cited by the Home Office:

- 66% of adults in the UK now own a Smartphone and 81% of them use it to send emails;
- The proportion of consumers in the UK using internet telephony services tripled from 12% - 35% between 2009 and 2014; and
- 19 billion online instant messages were sent in 2012, compared to 17.6 billion text messages [47]

An increasing trend is the use of online instant messaging which, even in 2012, replaced text messaging as the dominant form of messaging.

Law enforcement capabilities in relation to communication has traditionally been focused on landlines and mobile phone usage. The regulation of requesting
communications content is currently under the Regulatory Investigatory Powers Act 2015 [2]. The scale of these communication records requests is huge. Under data obtained by Freedom of Information Requests, the Big Brother Watch detailed more than 730,000 requests for communication data between the period 2012 and 2014 from police forces across the UK [48]. This number has since been increasing. The Head of the Interception of Communications Commissioner’s Office (IOCCO), told the Joint Committee in oral evidence that:

“Around 500,000 requests for communications data are made on an annual basis”. [49]

This information is clearly important to the authorities:

“It is used in 95% of serious and organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division and has been used in every major Security Service counter-terrorism investigation over the last decade.”[50].

Although it should be made clear that the majority of requests for communication data are not for serious crime.

Law enforcement have consistently argued that they have a ‘lost capability’ which is the subset of communication data which shows what device is connected to a particular internet service, such as an Internet messaging service like ‘WhatsApp’. There used to be, prior to DRIPA [8], no requirement for ISPs to retain this communications data and traditionally ISP only retained data that had a business use. Once law enforcement has identified a service that the person has accessed, they are then able to approach that organisation directly for information. It is this capability gap that ICRs seek to address i.e. approaching ‘WhatsApp’ that a communication took place on a certain day and time to ascertain further information. However, as previously explained this capability already exists in DRIPA.
Rationale

The Home Office has listed four main objectives for the operational requirements of ICRs. These are:

1. to identify the device that has sent a communication online;

2. to identify the communications services a device has accessed;

3. to identify the accessing of illegal online services e.g. to access illegal terrorist material or for the purposes of sharing indecent imagery of children; or

4. to establish the use of wider services of investigative value e.g. travel; [47]

In reality, these four objectives could be further distilled into two, as the last three are broadly similar. Thus, ICRs are concerned with identification of device and identification of services accessed. These two objectives will be analysed critically.

Breakdown of crimes

The breakdown of the crimes that law enforcement is accessing under RIPA [2] gives us an indication of the type of crimes that law enforcement is using communication data to investigate. This information shows that the major three crime categories are offences against property, drugs and sexual offences. What we cannot draw from this data is the more interesting question of ‘what value was the communication data to the investigation’. This question has not been satisfactorily answered in any of the evidence presented in the public domain.
Figure 2: Breakdown of 100,000 Communications Data Applications submitted under section 22(2)(b) RIPA by Crime Type [51]

* Other offences category (inc. public order, terrorism, traffic (serious & fatal accidents), corruption and cyber crime offences).

It should be noted that the examples used in the Operational Case [13] do not reflect this breakdown shown in figure 2, mostly focusing on fraud or child pornography – which are the some of the smaller categories in the above breakdown. This in some ways undermines the operational case examples as they are not representative of the normal requests for communication data.

The type of communication data that law enforcement is interested in can be shown by the type of communication data that was gathered under 300 interception warrants (note that interception warrants allow access to content). These were banking apps, travel services and mapping services (see figure 3)
This is an interesting portrait of how law enforcement is actually using the intelligence gleaned from communications data. The data is used more for intelligence leads than incriminating evidence.

**Identifying a device that has sent a communication online**

A main operational aim of law enforcement is to identify who has sent a communication i.e. in an online child sex exploitation case. This is done by what is known as, IP address resolution. IP addresses are the unique number that identifies a particular device and underpins the delivery of data over the Internet. Figure 4 below shows an example of how ICRs could be used in a potential investigation in identifying a device.

<table>
<thead>
<tr>
<th>Online service</th>
<th>% of cases service detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Maps</td>
<td>56%</td>
</tr>
<tr>
<td>Online Commerce Website A</td>
<td>37%</td>
</tr>
<tr>
<td>Online Commerce Website B</td>
<td>31%</td>
</tr>
<tr>
<td>Banking Services</td>
<td>27%</td>
</tr>
<tr>
<td>Travel Services</td>
<td>15%</td>
</tr>
</tbody>
</table>

Figure 3: Most prevalent accessed applications on 27 seized mobile phones [52].
Figure 4: showing how identifying a device could be useful in law enforcement investigation. [72]

IP address resolution is not as simple as this suggests. IP addresses were developed before the exponential growth of the Internet, and it soon became obvious that we would run out of IP addresses. A pragmatic solution to this was the use of Network Address Translation (NAT) and Port Address Translation (PAT). This enables a single public IP address to hide a large number of private IP addresses. A single public IP address can reveal as many as 5000 other uses.
Figure 5: Example of Communications Data held by CSPs for internet based communications [53]

This prevents a major problem for law enforcement as they need to narrow down that large number of private addresses. This is possible with other uniquely identifying information, such as port numbers and timestamps (see figure 6). However, a lot of this potential identifying information is not held by communication providers, who normally only retain data for billing and business purposes (see figure 5). This is the capability gap that ICRs seek to address (note previous comments on this power already existing in the Counter Terrorism and Security Act 2015 [10]).

Figure 6: Example of what an Internet Connection Record could look like [54]
There are a number of techniques that can be used to obfuscate the identity of a device which will negate the use of ICRs - these will be discussed latter.

The critical issue is will this information work for IP address resolution? Certainly, the Danish Experience with session logging, found that IP address resolution was an extremely difficult issue to resolve. The UK model is different from the Danish model but these same difficulties, particularly in relation IP addresses, are still huge potential problems (see Danish Experience). What is clear is that the guidance that the Home Office released in its draft Code of Practise [12] makes clear that this issue is complex and draws back from the idea that it is possible in all cases, especially in areas of shared IP addresses [54].

We should also recognise the limitations of device recognition enable by IP address resolution. That is, it does not identify an individual. Indeed, many communication platforms may be shared in the family or workspace, so simply identifying the device should not be confused with identifying a user.

**Identifying a service a device has accessed**

Law enforcement often wishes to know the website or service a person is accessing. From this they are able to build intelligence i.e. visiting a flight booking service means a person is likely to be booking a flight and travelling. Alternatively, accessing a popular messaging app, such as WhatsApp, means that the individual has likely sent a message to someone. Figure 7 below, shows how this information could be used in a missing person case.
There are two important aspects here; the first is that visiting a site may give vital intelligence i.e. visiting a travel website, or even evidence of visiting an illegal website - as in child pornography cases. The second aspect, is that it enables law enforcement to approach the relevant service directly. For example, if law enforcement approached a leading social messaging website, like Facebook, with a general request; ‘does this person use this site and can we see the records’, they would very likely be turned down.
However, if they are able to approach a service, with ‘this is your customer and he accessed this service, on this day and at that this time’, they are far likelier to get co-operation.

Difficulties

The major question to consider, is the utility of the value of internet connections. One of the major issues is the reality of near permanent connection for services like Twitter and Facebook. The very nature of these applications that enables them to alert you to messages and updates, requires near permanent connection, yet that does not mean that the person is actually using that service 24 hours a day. The argument from law enforcement has been, that for example, in a missing person case, this allows them to then make enquiries of the social networking provider. This does seem a very narrow illustration and in the broader examples of criminality, the utility of knowing that an individual was connected to the ‘BBC News’ for instance must be questioned.

Andrews and Arnold in their written evidence to the Joint committee make the point that many of these connections, using TCP but also SCTP (Stream Control Transmission Protocol) and MOSH (Mobile Shell), can potentially keep open connections for ‘hours, days or even years’ [55]. Thus, permanent connections, has certainly become the norm in recent years and the point they make in their evidence is that an internet connection might be logged when it has actually been used for several months or longer.

Potential for Abuse

It should be emphasised the very real danger in using ICRs is that they are open for abuse, accidently or in the following example deliberately. As Adrian Kennard demonstrated:

I did a blog post today, and anyone who reads it will find they have accessed Pornhub because there is a tiny one-pixel image in the corner. They do not know that, but it will appear on the Internet connection record if they access my blog. That was deliberate, but there could be lots of things on websites,
advertising networks and so on, that will create all sorts of misleading and confusing data even without someone trying to be misleading [56]

It would be very difficult to refute such an allegation showing the potential for abuse in the use of ICRs. There would need to be careful evidential standards if such evidence were to be used in a criminal court.

Distinguishing between communications data and content data

One of the key aspects of ICRs is that they should only allow law enforcement to access the services that you used and not the content. In simplistic terms, this is that they should allow law enforcement to see that you have accessed the NHS website but not what pages that you looked at. The Home Office describe it as the ‘who’, ‘where’, ‘when’, ‘how’ and ‘with whom’ of a communication but not what was written or said [57]. Thus communications data is information about the communication and not the communication itself. The then Home Secretary herself made explicitly clear, as noted by the Science and Technology Committee, in a statement to the House of Commons in 2004:

Some have characterised that power as law enforcement having access to people’s full web browsing histories. Let me be clear—that is simply wrong. An internet connection record is a record of the communications service that a person has used, not a record of every web page they have accessed. If someone has visited a social media website, an internet connection record will only show that they accessed that site, not the particular pages they looked at, who they communicated with, or what they said. It is simply the modern equivalent of an itemised phone bill [58].

This is a clear statement of intent, reflected in associated amplifying literature to the Bill, that only communications data pertaining to the service, and not its content, is to be captured by ICRs. However, many witnesses to both the Joint Committee and the Science and Technology Committee expressed concerns about the feasibility of this.
The problem with this view is that it represents an over simplified view of how the Internet functions. The Internet is not a single application, but for the typical user a number of applications are running simultaneously. This makes it very difficult to separate what is communications data and what is content data.

The ability to track all of this data would be an enormous undertaking and probably only possible by deep packet inspection – which is expensive. The Home Office witnesses to the Science and Technology Committee maintained that this would be possible. They argued that extensive consultation had taken place with industry to ensure that this was technology feasible. A statement that the larger communications providers, such as BT, concurred with.

This raises an interesting question as some of the ISPs can be very small and might not be willing to invest in this type of technology. The comment in the Science and Technology Report is telling in this respect:

*The Home Office indicated that “we will certainly not place obligations on every one of [the “200 or 300” communications service providers]. [59]*

There could be a variety of reasons for this. The cost of deploying the technology for a small ISP might be cost prohibitive for the Government (ISPs are entitled to claim all reasonable expenses back at 100%). The majority of users of the net, may be using just a few large ISPs. There is a suggestion that the ISP architecture in the UK means that the majority of communication passes through only a few networks at some point, and these would be the ISPs that would be concentrated on. This is extremely likely as British Telecom for historical reasons owns much of the infrastructure that is used. Certainly these issues raise interesting future research lines. However, given the operational secrecy and the unwillingness of ISP to discuss this, it will be an extremely difficult research problem to fully resolve.

Whilst it seems that the differentiation between communication data and content data is problematic, it does not appear to be impossible. The Home Office and the major
ISPs are in agreement on this, although (understandably) there is no explicit detail on how this will be done. It is likely to involve deep packet inspection but again it remains unclear as to what extent this technology would need to be deployed across all ISPs. Certainly, session logging on the extremities of the network, as done in the Danish model, has not proven to be very satisfactory.

An interesting argument is that communication data may be actually more useful than content data. Content data can be very resource consuming to analyse. Whereas communication data can be mined and filtered, in greater numbers and less resources, to reveal some very private information. Liberty, the civil liberties NGO, made this very point in their written submission to the Government [69]. They use a number of powerful arguments to illustrate this, including the Intelligence and Security Committee when looking at GCHQ:

_We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications._ [70]

Access to content data has a far higher threshold than access to communications data on the basis that it is perceived to be more intrusive. However, with the increasing ability to mine complex data sets, it could now be argued that communications data is actually more intrusive.

**Experiment in the value of ICRs**

One of the contributors to the written evidence of the Science and Technology Committee was by Tim Patton, a software developer [60]. He sought to recreate the collection of ICRs against the three operational cases made for ICR’s, namely:

1. _to identify the device that has sent a communication online;_
2. _to identify the communications services a device has accessed;_
3. to identify the accessing of illegal online services e.g. to access illegal terrorist material or for the purposes of sharing indecent imagery of children; or
4. to establish the use of wider services of investigative value e.g. travel

His methodology, was to enable his firewall to collect the address and port data from each connection for just one day. This has the result of collecting the packet for the first packet of each connection. Whilst the exact mechanics of how ISPs will conduct the collection of ICRs, and this may vary from ISP to ISP, this is likely to be from some deep packet inspection. Whilst the collection is different, the data collected would in principle be the same. So whilst there are a number of criticisms can be levelled at this individual experiment, it does serve as a useful starting point as to the reliability and use of data.

An example of the data collected is shown in figure 8. This shows time, the protocol, the source address and port, the destination address and port.

![Figure 8: communications data from obtained form firewall](image)

This corresponds to the examples of communication contained in the Draft Code or Practise [12]. In the case of being able to identify the IP address that matched to the ICR entry, the practitioner had mixed results. Whilst he was able to identify an email sent to his email account using his desktop computer, he was unable to the same when using his Android based mobile phone. As the writer notes the ‘trend is towards more mobile device usage and away from desktop computers’.

The author also highlighted the difficulties in using ICRs to determine which services he had used. Whilst the ICR could identify an email account (of obvious use to law enforcement), it did not not show the webmail services he used (Yahoo and Gmail). Whilst ‘Google’ was highlighted, the most interesting aspect was the high showing of ‘Akamai’. This is Content Delivery Network (CDN). The aim of a content delivery
network is give high performance and availability to hosted web pages. This is done by using a server that will host content for other user’s which is located nearest to you. Thus, if you request the web page of the “New York Times” for example, then that content may well be hosted by a UK server acting as a CDN. It is also interesting to note that none of the messenger apps the user used (Skype and Wire), showed up. Whilst this experiment of N + 1 can be criticised from a number of objective criteria such as sample size, length, technology used, this should not overlook the fact that the data he collected – which is as close to what we understand ICRs to be, was in many cases not that useful and did not fully meet the stated operational aims of the ICRs.

What is needed is a larger study or comparative use of ICRs, which we will look at in the next chapter – The Danish Experience.

Summary of Main Points

• People have changed the way they communicate with a far greater reliance on smartphone and using intent based communication. Email is the dominant form of messaging.

• There are a huge number of data requests by law enforcement and this is growing – some 500,000 in 2015.

• Law enforcement’s main concern with communication data is IP address resolution and identification of internet services accessed.

• Most communication data requests relate to property, drugs and sexual crimes.

• IP address resolution is extremely complex, and whist ICRs are useful, it is unclear they will greatly improve in aiding in resolution.

• Near permanent connection, particularly to social networking sites, can negate the value of what information ICRs are able to provide.
• There is huge potential for abuse in showing which sites an individual has visited.

• Communications data may in fact be more intrusive that content data.

Conclusions

A well argued and credible case for the introduction of ICRs would be for their purpose to be clear. The two clearly stated purposes of ICRs, namely IP address resolution and identifying the services a person has accessed, are not overwhelmingly solved by their introduction. IP address resolution is more complex than it appears, and access to services has the potential for abuse and distortion through permanent connections. There is also a credible argument that communications data is more intrusive and revealing, than content data. Much more detailed research needs to be done on these issues once the Bill becomes law – ultimately to see if ICRs comply with their original purposes in a useful way.
The Danish Experience

Introduction

The Danish experience shares many similarities to the aims of what ICRs aspire to achieve. The scheme ran in Denmark from 2007 until 2014. The scheme was closed down due to the lack of usefulness of the collected data. The scheme will be outlined below, the various similarities and differences between the proposed UK ICRs and the Danish experience will be explored. The Danish experience has particular resonance as it is the only large scale example that offers a comparison to ICRs.

Overview

The discussion period between the Ministry of Justice and the ISPs as to what could be achieved, took 2 years. The requirements identified were for: - the source and destination IP address, source and destination port number, transmission protocol (i.e. TCP or UDP) and timestamp [61]. The original intention was for the the first and last packet to be logged but the alternative solution, which became the widespread solution, was to log the 500th packet at the boundary of the network.

A 2012 report by the Ministry of Justice, found that the retained records had been of little use to law enforcement, a finding which was concurred with by the Danish Security and Intelligence Service. One of the problems encountered was the sheer mass of data that was collected:

*In 2013, about 350 billion records about telecommunication were retained in Denmark (620,000 per citizen), of which more than 90 percent was due to session logging.* [62]

A further problem, highlighted in the written evidence to the Committee, was that the session logging could only identify devices that were connected to the ISP, such as a desktop computer. A mobile device, using a Hotel Wi-Fi, is not identified as the ISP and can only identify the hotel itself.
Comparison of the Danish Experience and the UK

Having the Danish experience was clearly an influential strand of evidence, and both Committees received evidence from the IT – Political Association of Denmark. The Joint Committee also heard oral evidence from Jesper Lund of the said organisation [63].

The most obvious similarity between the Danish and UK systems are their similarity of aims i.e. to enable device recognition and identify services accessed. Given that these aims are so simultaneous; the Danish experience is particularly valuable given its abandonment by the Danish Ministry of Justice. If we can clarify why the Danish experience was so unsuccessful, we can analyse if the UK system is able to circumvent those difficulties that beset the Danish model.

The first major difference is one of cost. The Danish model, as Jesper Lund argued, was far less ambitious and the cost of data retention was borne by the CSPs. Arguably, these businesses are always going to support the most cost effective solution as this directly impacts on business costs. The consequence of this decision, was that the cheaper solution of collecting the ICRs, at the ISP’s network boundary was chosen. When IP addresses are not shared this is not a problem, but where there is a sharing of multiple IP addresses, this can become a big challenge. In 2005, when the Danish project was being negotiated between the Danish Ministry of Justice and ISPs, the use of shared IP addresses was only a limited concern. The growth in the use of accessing the Internet via smart phones made this a very common problem. In the evidence presented, approximately 50% of records were not useful because of this problem with IP address resolution with shared public IP addresses [64].

Will the proposed UK legislation be able to overcome this? Firstly, we don’t obviously know as the the definition of an ICR is so broad ranging, and there is no stipulation by the government of how this is to be achieved. The UK model is different in that it is the intention, although not explicitly stated in the the Bill, that all ‘reasonable’ costs will be borne by the Government. Furthermore, before a notice is issued to a communications
provider, there is an initial discussion with law enforcement before the notice is issued. This makes for a far more flexible, albeit less transparent model than the Danish one.

This means that it is unlikely for the UK model to involve sampling the network at the boundaries. Given the ubiquity of smart phone ownership, it would seem inconceivable that a model would be introduced that could not distinguish between shared IP addresses. The UK model would depend on the ISP and is likely to involve deep packet inspection.

As Jesper Lund’s written evidence explores, overcoming this problem might not do much for the utility of ICRs. Whilst 50% of ICRs were not usable, for the reasons outlined above, the remaining 50% of collected ICRs should have been highly usable – this was not the case. It is not clear why the Danish Police and the Danish Intelligence services were not able to make use of the remaining data, but it is suggested that the amount of data collected – the proverbial ‘needle in the haystack’ was the problem. What is clear is that the Danish project was closed, not due to public concern but the accepted limitations of the system by the Danish Ministry of Justice themselves. This is quite a damming recommendation in that, if the collected data was of use in any way, a case would have been made for its retention. The self assessment by the Danish Ministry of Justice could find no recorded cases of its benefit in investigations.

The UK model of deep packet inspection may allow greater visibility on what services a user is accessing. However, what is not clear is the extent to which this technology is distributed across ISPs. The inference is that it is not widespread and it is probably not cost effective to install across all ISPs.

Given the concern over the Danish Experience the Home Office released a document titled ‘Comparison of internet connection records in the Investigatory Powers Bill with Danish Internet Session Logging legislation’ [15]. This was in response to the Joint Committees recommendation that they should publish a full assessment of the differences between the two models. The document seeks to show the core differences between them.
The report argues that the reimbursements of costs to communication providers will mean that they will not choose the cheapest option. In Denmark, this was the sampling of every 500th packet, which removed the requirement for deep packet inspection. Furthermore, the UK legislation will not specify how the collection is to be done. The UK notice is not issued to the CSPs without consultation, which takes into account what is feasible – with the CSP having a right of appeal to a Technical Advisory Board.

The Danish model collected data at the boundary of the network. The UK model intends to do this before IP Network and Port Address Translation (NAT / PAT) has been applied. The effect of this will be to allow greater IP address resolution, as this will allow data to be matched against a customers’ account. The Home Office in the UK, is already doing this under the Counter Terrorism and Security Act 2015.

The UK model has a very flexible definition of what constitutes ‘communications data’, whereas the Danish model was very specific as to the collection requirements. It can be argued that this gives greater flexibility in including data that allows identification of used services. The disadvantage of this is that, a legislative power is not clearly defined and thus is not explicitly limited.

Summary of Main Points

- The Danish model which ran from 2007 – 2014, is the nearest example of a similar scheme to ICRs. The trail was stopped because of the lack of usefulness of the collected data.

- The solution used in the Danish model was log the 500th packet at the boundary of the network.

- As a result of this method, a major problem was the use of mobile smart phones, which meant IP addresses could not be attributed. This was approximately 50% of the data.
• The remaining 50% of data was also not useful – although it was unclear why this was but it suspected that it was the sheer volume of data.

• The Home Office argues that the UK model can overcome these problems. This is primarily done by using deep packet inspection and by having a more flexible definition of what constitutes communications data, which will vary from ISP to ISP in the ‘retention notice’.

Conclusions

The historical maxim that ‘there are no new lessons, just painful old ones’ has the potential to apply here. The Danish experience highlights the large problems that collecting and logging this type of data presents. The impact of the Danish experience resulted in both Parliamentary scrutinising committees asking the Home Office to produce a document to show where and how the UK model is different. However, that said, till the scheme is operational, it will be difficult to assess the ability of the UK scheme to overcome the problems that have been highlighted by the Danish experience.
Avoiding the Impact of ICRs

Introduction

The two important principles behind ICRs are; the ability to correctly identify devices and to see what services those devices have been using. If ICRs are to be an effective tool for the law enforcement community, then the ability to evade these two aims should be difficult. In this chapter we will look at some of the ways individuals can bypass these aims, whether by deliberate effect or by simply using services that defeat these aims, even if they are unaware of them. The majority of these techniques are well known, are currently in use, and do not require individuals to be ‘technologically savvy’.

With the exception of encryption, the majority of these techniques are not in use by the wider population. The impact of the Investigatory Powers Bill has not really entered the public consciousness, so these techniques are therefore not widely utilised. It should be noted that organised criminality and terrorist groups already deploy many of these measures, so the impact on these groups through ICRs is likely to be minimal, unless they are careless. What remains to be seen is whether individuals adopt these methods to avoid the potential impact of ICRs, or as a consequence of a greater awareness of on-line security. The unanswered question is ‘does the ability to circumvent the impact of ICRs undermine their introduction?’

Virtual Private Networks (VPNs)

A VPN allows a user to send his data via a third party before routing to an ISP. This means that the data the ISP receives is encrypted (see encryption). Thus, any deep packet inspection of your data will be unintelligible to any observer, unless they had the means to break the encryption. VPNs are used for many perfectly legitimate purposes, such as allowing a travel salesperson to communicate securely with his head office.
Using a VPN would clearly frustrate the purpose of ICRs. Whilst VPNs do not provide anonymity they do provide confidentiality. That is, the source address and destination address would be still be visible but the contents of your traffic would be encrypted.

VPNs are very easy to set up. VPN providers are free or can be purchased at low cost. Individuals are reliant on the integrity of the VPN provider. If this VPN is provided in a third country, then it would be further removed from UK law enforcement jurisdiction. A potential restriction on the use of VPNs is that they can reduce the speed of your internet connection. This limitation alone, for many people, would negate them from using VPNs.

The Bill itself, nor the Government supporting documentation associated with the Bill, mention VPNs, or their impact. The Parliamentary scrutinising committees heard both oral and written evidence from many sources, that VPNs would reduce the impact of ICRs but both committee reports made little reference to this fact in their final reports.

Encryption

The use of encryption, and the increasing use of encryption, is the most major threat to the ability of the ICRs to achieve their stated aims. If we consider the most common use of encryption used in communication between members of the general public, it is encrypted social messaging such as ‘WhatsApp’ or ‘iMessage’. This is the most common form of messaging, and is overtaking text messaging as the most popular form of messaging. Ordinarily, the average user is not using encryption in emails, although such tools are easily available.

These apps use what is known as end to end encryption. This means that only the end users have the cryptographic keys to encrypt and decrypt the messages sent between them. ISPs, servers and eavesdroppers can only read the messages if they are able to break the encryption, a very difficult task. However, what an ICR would still be able to record is that you have used an instant messaging app. This is itself would potentially be extremely useful, circumstantial evidence i.e. when messages were sent etc.
Another important factor to consider is that the metadata created, in using an app like WhatsApp, is stored by the company. Although, because of the encryption, the messaging company is unable to read those messages, the information held on whom you talked to, and when, is recorded. This can be used as very powerful evidence. It is beyond the scope of this project to define when law enforcement could access this metadata from the messaging companies, or the jurisdictional challenges if the company is based overseas, but it should be noted the effect that increasing encryption is having.

We are certainly seeing the increase in the spread of encryption. Many web pages are now using HTTPS (Hyper Text Transfer Protocol Secure) which were previously the preserve of banking websites only. In terms of impact on ICRs this will only show what websites you were looking at but not the the content – which is within ICRs terms of reference anyway.

What the most pressing aspect of encryption is having, that will effect ICRs, is that users of technology are having a far greater awareness of the issues of privacy and confidentiality than before. It is this new attitude to personal data that may well frustrate the efforts of ICRs than encryption itself.

**TOR- The onion router**

One of the many ways that the impact of ICRs can be circumvented, is by using TOR or similar applications. The crucial importance of TOR is that it does not provide confidentiality. However, it does provide anonymity. This means that TOR’s aim is to hide a users’ location and identify from anyone conducting surveillance, or traffic analysis, of the net. The practical effect of this, is that an individual cannot be traced by their IP address. TOR does this by connecting users through a series of VPNs. This means that anyone conducting traffic analysis (which is what ICRs effectively rely on) is unable to know who is sending or receiving information. This is more powerful than encryption, in certain circumstances, as encryption only protects the contents of your
message but the source and destination address are visible to traffic analysis. Simply knowing who is talking to you can be very useful intelligence on an individual.

TOR is already widely used by terrorist and organised criminality and it does not require a high degree of technical knowledge to set up – and is free. It should be noted that TOR has perfectly legitimate purposes, such as business people travelling aboard or individuals wishing to evade government sensors.

TOR at the present is a fairly niche application, although there is circumstantial evidence that evidence has increased since the Snowdon revelations. The more users who use TOR, the greater the effect of its anonymity. A few users using the service are conspicuous and will stand out, whilst a larger number of users of TOR will ensure more anonymity. A consequence of the introduction of the Investigatory Powers Bill, is that we may see greater use of TOR by either legitimate users concerned about their privacy, or criminality. Either way, a simple and free downloadable application would defeat the primary purpose of ICRs i.e. being able to identify users from their traffic. The detriment of using TOR at the moment is that it does slow your connection speed.

The use of TOR should be a real concern to law enforcement. The introduction of ICRs is reliant on there being no greater appetite for its use amongst the wider public. We will not know the answer to this question until the Bill becomes an Act.

**Wireless Mesh Networks**

The difficulty in legislating in areas of rapidly changing technology, is that the emergence of technologies can bypass your intentions. Wireless Mesh Networks is one such example. These use small radio transmitters that function in many ways similar to a wireless router. Individuals use their device as transmitter which allows data to be transported from device to device until it reaches its destination. This is an emerging technology but is useful in small areas where there may be no internet connectivity. There are wide practical applications for this such as extending Internet services to school children in poorer countries where there is limited Internet connectivity. Using
such a mesh network would mean that individuals would be able to bypass communication providers, and hence the inspection, that enable ICRs to be captured. Firechat is a commercial application of this, and has been used in civil disturbances, or in protests where the Wi-Fi was turned off or mobile phone signal blocked [71].

Emerging technologies such as wireless mesh networks, may soon outpace the legislation that is trying to stay current. Wireless Mesh Technologies would defeat ICRs as there seems little way of enabling the proposed legislation to be able to bring ICRs to this area.

**Protest Browse**

One of the aims of ICRs is to see what services you are accessing, thus enabling law enforcement to build up intelligence i.e. visiting a flight booking service indicates a willingness to travel. However, an individual can obfuscate this information by visiting, for example, 9 random sites for every one an individual has a legitimate reason in. Whilst this is time consuming for an individual, it does demonstrate a simple obfuscation technique and one that is not beyond automation. There are already similar programs such as ‘TrackMeNot’ doing similar automated searches for Google thus obfuscating users’ web searching history.

**Summary of Man Points**

- There exists a number of different ways, the aims of ICRs could be frustrated, deliberately or unintentionally.

- These methods are already in use by serious criminality and terrorist organisations but probably are less used by ‘everyday users’. There are legitimate reasons for potentially using these tools.

- VPNs are the most common way of frustrating ICRs, increasing encryption will also further guarantee content.
• TOR is a very powerful anonymising tool that could become more widespread in the UK following the introduction of the Bill into law.

• New emerging technologies, such as Wireless Mesh Networks, which bypasses ISPs could make make ICRs ineffectual.

• The effect of protest browsing or other obscuration techniques can be used to obscure what services you have used.

Conclusions

ICRs may well be effective under current communication patterns. However, there are simplistic measures that can be adopted to circumvent ICRs effects. The reality is that organised criminality and terrorism are probably well acquainted with these countermeasures. Furthermore, the adoption of these methods may well increase amongst law abiding citizens concerned about their privacy. None of the techniques mentioned are beyond the reach of the everyday user. The existence and take up of these avoidance methods does cast doubts on the feasibility of ICRs.
Suggested Future Lines of Research

Introduction

Given that the Bill has yet to be enacted, much of this dissertation's research will also be applicable when the the Bill becomes an Act. The real value of any future research will be, no doubt, on the actual use of ICRs in practise. This will show whether the potential concerns and challenges raised by this research have materialised in its practical application.

ICRs are just one part, albeit central part, of the Bill but the length and depth of the Bill will occupy many potential research lines for many years to come. What follows below is a number of research lines that deserve attention.

IP address resolution

One of the central tenants for the introduction of ICRs was IP address resolution i.e. to be able to link a communication to a device. Evidence before the Parliamentary Committees from law enforcement saw this as a key aim, but there were also witnesses who noted this was a far more complex area than many imagined, particularly where IP addresses are shared. This is especially common with mobile smart phones. The Danish experience showed, with session logging, they were not able to overcome this difficulty. A productive area of future research would be to ascertain how effective ICRs were in IP address resolution. The draft code of practise, released by the Home Office, following the publication of the scrutinising Parliamentary reports, appears to take a more pragmatic tone on IP address resolution and the difficulties this causes:

In the current technological environment this is often not a simple task and applications to acquire communications data for this purpose must consider the associated complexities [61].

If IP address resolution was not better enabled by ICRs, then a major argument for their introduction would no longer exist.
Utility of ICRs

A future research line once the Bill becomes law, is the actual utility of ICRs. Evidence presented to the Committees showed that law enforcement regarded these as essential in their work. However, aside from specific examples of child protection, there was no empirical evidence to support these claims. This is the million-dollar question for ICRs ‘what is their actual utility in investigations’ or perhaps ‘given the effort, money and intrusion of ICRs, will the investigative value they add outweigh these factors’. At present, we simply don't know what value this type of communication data is to law enforcement. This would be a very large research area, and a very complex one. However, it would seem a very important one. With ICRs, we are granting the Government and law enforcement very intrusive powers without fully knowing the evidence basis for granting those powers.

Such a study may well reveal that ICRs are more important in investigating one type of criminality more than another. Such a study may well help to ascertain the extent to which criminality is using methods that frustrate communication data collection. The use of evidence based research in this area would inform the law enforcement community and the wider public of the actual utility, and continuing utility of ICRs.

Avoidance Methods

One of the research areas already discussed, was the use of avoidance techniques such as VPNs, TOR and increasing encryption to circumvent the impact of ICRs. Whilst these techniques are known about, with the exception of encryption, they are not necessarily widely utilised. A future research area would be to see the increase in the use of these methods following the introduction of the Bill. There is anecdotal evidence that, post-Snowdon, there was an increase in these methods. Specific research in this area would add value, not least if the evidence suggests their use is becoming so widespread to seriously undermine the effectiveness of ICRs. If this were the case then the utility of ICRs would be questioned.
Definitions

The current definition of what an ICR actually is has been deliberately left very open, thus allowing the concept of ICRs to be ‘future-proofed’. There have been strong indications in both the Bill, and the supporting documents, as to what data this is likely to entail. A difficult, future research line would be to look at how this definition changes over time. This line of research would also be used to ensure that any changes to the definition are not beyond what the Bill allows for – or the ‘spirit of the Bill’. By defining ICRs in the very broad way they have, and ensuring that ISP keep the notices they receive secret, there is a real danger that ICRs become a more expansive data set than originally intended in the Bill.

Accountability and Oversight

The Bill brings in new ways of how the retention notices will be overseen. This has not been touched upon in this research but is part of the broader implications of the Bill. This would be a fruitful line for future research.

The integrity of collected data, both by ISPs and the police, was raised as a concern by some witnesses before the Parliamentary Committee. The Bill contains specific provisions giving obligation to protect that data. A future research line would be to see if these were adequate and to analyse any data breaches in this area.

Conclusions

Given the broad nature of ICRs, and their implications, both technical and social, there is a wealth of potential research lines for future researchers. Given the intrusiveness of ICRs, this research work would have huge social value. Given the paucity of data as to the utility of communication data, any work which is able to show empirical evidence as to their utility would add greatly to the understanding of this topic.
Conclusions

The Context to the Bill

The introduction of ICRs is a consequence of both changing technology and patterns in the way we communicate. The Bill aims to bring together a number of disparate areas of legislation and further in doing so provide clearer authorisation and oversight arrangements. ICRs are a central tenant to the Bill. It has been restated that this will reintroduce capabilities that have been lost. However, careful analysis reveals that these capabilities exist already in legislation, so this claim is not valid.

Definition

The biggest potential criticism of ICRs is the lack of clarity over what exactly is an ICR – aside from being communication data. This is a doubled-edged sword, in that this broad definition allows for an element of flexibility that future-proofs the legislation, meaning that the legislation is not continually revisited. In this research we have suggested that an appropriate analysis in this instance is that the ICR is viewed as a model. Thus, the ICR is seen as more as a principle of collecting communication data than an absolute. The danger in this model is that it allows the Government to incrementally increase the data, far beyond which that it is originally intended. The fact that retention notice issued to ICRs are not for disclosure means that the onus is on Parliamentary scrutiny of the legislative implementation and the efforts of researchers (with the difficulty in obtaining this data) to ensure that this is monitored. A potential solution to this is to allow Parliament to revisit ICRs specifically, as opposed to the legislation in its entirety, if it was felt that the definition of ICR was needed to be expanded. In this way the definition of an ICR could be far more explicit.

How an ICR works

ICRs are primarily concerned with the law enforcement community, as opposed to the intelligence community. A distinction is made between access to communications data and the power to retain communication data. The retention of communications data is only possible by a notice by the Home Secretary, and is for a maximum of 12 months.
There is a consultation with the telecommunications provider before before such a notice is issued. In issuing the notice, the cost and technical feasibility is taken into account. Therefore, a retention notice may well differ between telecommunications providers. It appears that not all of the UK’s ISPs will be targeted with notices because ISPs must not disclose that they have been served a notice.

Purpose of ICRs

People are communicating in different ways, with far greater reliance on Internet communication. The purpose of ICRs is to identify devices which have sent communications and identify services that have been accessed. Communication data is increasingly used by law enforcement in investigation of crimes, although currently there is little empirical data as to its exact utility.

There are major difficulties in identifying a device that has sent a communication online. This is due to the sharing of IP addresses, with a public IP address hiding potentially thousands of IP addresses. ICRs aim to get around this problem by narrowing this number down with further data captured by the ICRs such as port numbers. Later documentation released by the Home Office [12] seems to acknowledge that this problem is in fact far harder than originally stated. It should also be noted that legislation, dealing with IP address resolution was introduced in s 21 of the Counter-Terrorism and Security Act 2015 [10].

Another aim of ICRs is to identify services accessed online. This is to identify intelligence leads for law enforcement i.e. banking accessed, willingness to travel etc. One of the difficulties here is the near permanent connection made by devices to some sites, particularly social media sites. The value of this information can be questioned, although critics to this view argue that it allows you to approach those social media organisations for further investigative leads. There is potential for abuse of this, by for instance hiding images on a visited website, such as from a porn site. This creates potential for false information and potentially questions the reliability of evidence.
From comments made in evidence, by the Government, it would appear that not all ISPs will be issued retention notices. This raises interesting questions of whether smaller ISPs will escape scrutiny or if the UK ISP architecture is such that all communication eventually passes through a limited number of ISPs.

Danish Experience

The Danish experience of internet logging sessions was not a success. Indeed, the self evaluation by the Justice Ministry of the scheme led it to being stopped. There were two main reasons for this. IP resolution was not possible with shared public IP addresses, particularly in relation to mobile phones - this was for over 50% of records. Secondly, the remaining data was that was collected was not usable by law enforcement in any meaningful sense.

The UK model differs from the Danish one, primarily in how the data is collected and at what point. Proponents of the scheme, argue that this will be a significant change from the Danish scheme and will provide far better results. This should be evaluated and reflected in future changes to ICRs.

Whilst certainly, the UK has world class expertise in the interception of communications, there are potentially serious flaws in the UK model. Certainly the Government in the release draft Code of Practise appeared to be acknowledging the problems in IP address resolution – which was one of the key aims of ICRs.

Avoiding the Impact of ICRs

One of the biggest problems with the introduction of ICRs is the relative ease they can be avoided. The prime means for these have been outlined but the key point is the ease of which they can be circumvented. There is no empirical data that people in general are using these methods to avoid the potential impact of ICRs or interception more broadly. However, the increasing use of encryption as the default norm across many communication services show there is a greater appreciation of security and privacy
amongst the general public. Whilst the Investigatory Powers Bill is probably not high in the public consciousness at the moment, that is not to say that could not change. Certainly organised crime and terrorists take measures when communicating to mitigate interception. It remains to be seen if there is a wider application of these method. What is clear is that a wider intent to avoid ICRs would not only be easy but if done in any significant way, would totally undermine the whole point of ICRs.

**Final Concluding Remarks**

The Investigatory Powers Bill dealt was always going to be a controversial piece of legislation in that it is concerned with the privacy of the individual and the powers of government. ICRs are a central plank of the Bill and this research has focused primarily on what ICRs actually are, their purpose, and the challenges in making them effective. ICRs are challenged are many fronts. The sheer pace of change in technology and the way people use the Internet makes legislating in this area very difficult, if the legislation is not to quickly become redundant. ICRs with its very board definition aspires to overcome this. This had made it difficult, although not impossible, to predict the data set that will be captured. This is far less than full interception, but communication data is still revealing about the individual, and with ‘data mining’ may be more so.

There appears to be in many ways some over simplification in the presentation of what ICRs will be able to achieve. Whilst communications over the Internet can be simply defined, the reality of those protocols can be quite complex. The difficulties in IP address resolution with public IP addresses is an example of this. Therefore, if introduced, the practical reality of what level of utility they provide to law enforcement will be critical. Given the ‘low bar’ set by the Danish experience it may not be as useful as perhaps the evidence has been presented.

The premise that ICRs give back to law enforcement powers they have lost, is misleading. This is because many of the powers already exist in desperate pieces of legislation. The case of the IP resolution in the Counter-Terrorism and Security Act 2015. Whilst the Bill brings all these powers together, and keeps some for legislation
that is time defined, such as DRIPA, there is little new outside obligation to retain the data.

The Bill faces many challenges ahead. The recent ruling by the European Court on the provisions of DRIPA and its applicability only to organised crime, may well drive ‘coach and horses’ through the Bill. There are technology issues to address with the practicalities of the system, and there is the ease with which the objectives of the ICRs can be easily avoided.

The Bill and the subsequent Act will most likely be subject to much scrutiny and research in the future. This first study of ICR is a useful first step in that scrutiny.

Value of this research

This research has helped to highlight the problems in definition of ICRs. Whilst others have also raised this point, this research has been a systematic analysis of why the definition of this term as been so difficult. This research has also highlighted that many of the powers already exist in other pieces of legislation. This has been a key finding and one not addressed in Parliamentary scrutiny. The argument that ICRs retain lost capabilities has been proven to be inaccurate, and has not been highlighted in other commentary so far, to my knowledge.

By comparing the Danish experience to what we know of the UK model, this research has shown that the difficulties in getting meaningful data from captured communications data can be difficult. The UK model may get around some of these difficulties through its methodology but this research has highlighted that are concerns about the utility of some of the data that is captured. Finally this research has added to the literature in showing that ICRs can easily be evaded through use of VPN and anonymising tools, such as TOR.
Bibliography


4) UK Parliament, *Communications Data Bill*, 2010-2011

5) Case C-293/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014], ECLI:EU:C:2014:238

6) OFCOM, *Communications Market Report* (OFCOM.org.uk), 6th August 2015 [27 July 16].

7) House of Lords, House of Commons, Joint Committee, *Joint Committee on the Draft Investigatory Powers Bill*, 3 February 2016, HL 93, HC 651


21) The Investigatory Powers Tribunal, Ms. Jenny Patton and other vs. Poole Borough Council, IPT/09/01, 6 November 2009


28) UK Parliament, Investigatory Powers Bill, 2015-2016, s 72 (2)


31) UK Parliament, Investigatory Powers Bill, 2015-2016, s 77 (2)


49) House of Lords, House of Commons, Joint Committee, *Joint Committee on the Draft Investigatory Powers Bill*, 3 February 2016, HL 93, HC 651, Oral Evidence, Qu 48, Jo Cavan, Head of the Interception of Communications Commissioner's Office,


51) Interception of Communication Commissioner’s Office, *Senior Responsible Officer Circular (4)*, Breakdown of communications data applications under s22(2) (b) RIPA by crime type, 20 November 2015, [17 March 16],
http://www.iocco-uk.info/docs/SRO%20Circular%20(4)%20-%20Breakdown%20of%20applications%20under%20s22(2)(b)%20by%20crime%20type.pdf


56) House of Lords, House of Commons, Joint Committee, *Joint Committee on the Draft Investigatory Powers Bill*, 3 February 2016, HL 93, HC 651, Oral evidence, Qu 123, Adrian Kennard,


71) Wired, *Firechat will become a totally free mobile carrier*, 05 August 2015, [1 August 2016], http://www.wired.co.uk/article/firechat-full-mobile-carrier-free

Customs, and Richard Berry, National Police Chiefs Council,
http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB63.pdf