Coimisiún na hÉireann um Chearta
an Duine agus Comhionannas
Irish Human Rights and Equality Commission

MEMORANDUM

TO: **Mr. Justice John L. Murray**

FROM: **Irish Human Rights and Equality Commission**

RE: **Review of the Law on Access to Communication Data**

DATE: **13 June 2016**

MEMORANDUM

TO: **Mr. Justice John L. Murray**

FROM: **Irish Human Rights and Equality Commission**

RE: **Review of the Law on Access to Communication Data**

DATE: **13 June 2016**

Contents

Introduction

This Memo provides background information to the Murray Review (the **'Review'**) established in January 2016 to examine the legislative framework in respect of access by statutory bodies to communications data. The Irish Human Rights and Equality Commission (the **'Commission'**) highlights human rights and equality issues of concern in relation to the specific context of the Review.

The Commission was grateful for the opportunity to meet with you on 1st June as part of your Review. The following is a short summary of issues raised at our meeting:

- Finding the right balance between privacy and press freedom rights against the legitimate public interest in an effective crime prevention system, is one of the big human rights challenges for our generation. Failure to achieve the right balance has grave consequences for civil liberties.
- The professional privacy issue for journalists is a subset of the wider privacy issues engaged – 62,000 requests for individual's communications data or metadata were made over a 5 year period. This amounts to almost two requests an hour, mainly by An Garda Síochána. Fewer than 2% of requests for data were refused by the service providers. Record keeping is minimalist at best, and therefore there are significant issues in terms of the procedural element of the fundamental human rights raised, including the right to effective remedies.
- This is an issue which is unlikely to go away. Surveillance technology is outpacing the law. Therefore, this represents a great opportunity for the Review to make practical and principled proposals to ensure that any review of the legislation is informed by the relevant domestic and international human rights standards and is future-proofed to the greatest extent possible.
- The current legal framework is light touch, and not human rights compliant in that it lacks the necessary quality of law, well-resourced independent expert oversight at appropriate points in the process, and access to effective remedies where rights are infringed.
- Enhancing safeguards would serve to bolster public confidence in investigations and the wider criminal justice system, ultimately benefitting all stakeholders, including victims of crime.
- The Commission considers that the inadequacies in the current framework for data retention and disclosure call for root and branch reform. The combined impact of incorporating discrete protections at various stages could lead to a shift in culture.

At the outset, the Commission notes the Review's rather straitened Terms of Reference.[1] As such, this Memo is focused on the Terms set, but the Commission regrets that the privacy rights of ordinary adults and children fall outside the scope of the Review despite their private communications data being equally susceptible to retention, access and disclosure to third parties under the legal framework discussed below.[2]

[1] The Review is mandated: 'To examine the legislative framework in respect of access by statutory bodies to communications data of journalists held by service providers, taking into account, the protection of journalistic sources, the need for statutory bodies with investigative and/or prosecution powers to have access to data in order to detect serious crime, and current best international practice in this area.' See Department of Justice and Equality (2016) 'Statement by the Minister for Justice and Equality in relation to access to telephone records' [press release] 19 January 2016, available here.

[2] See Karlin Lillington, 'Journalists, this GSOC story isn't all about you' *Irish Times*, 21 January 2016 http://www.irishtimes.com/business/technology/journalists-this-gsoc-story-isn-t-all-about-you-you-know-1.2504162 –

''Only because successive data protection commissioners threatened to stop any call data at all from being retained, did the government shamefully sneak through legislation in the form of an amendment to unrelated legislation, before a near-empty

While this Memo primarily provides information specific to the Review, the principles of privacy protection and freedom of the press, detailed below, are also applicable in the broader context of surveillance. These are issues which are likely to be increasingly relevant for Ireland as the data protection framework changes at a European level,[3] and further data privacy cases are handed down by the Court of Justice of the EU.

The Commission also highlights the relevance of its equality mandate in the context of the Review. The necessarily covert nature of criminal investigations largely precludes any examination of whether statutory bodies' significant powers are always exercised in a lawful, non-discriminatory manner. A strong message that equality considerations are embedded in the practice of data accessing, for example as part of a statutory Code of Practice, would provide some reassurance. The Commission draws attention to the section 42 IHREC Act 2014 Public Sector Duty, which binds public bodies to have due regard to the need to protect human rights and eliminate discrimination in the exercise of their functions. This may be beneficial in terms of thinking ahead to avoid data access requests having a disproportionate impact on any one community or category of people.

Dáil chamber a decade ago. This however failed to raise the interest of journalists, media companies or unions, even when it was pointed out by privacy advocates here and internationally, that journalists themselves should be deeply concerned.

Call data are highly revealing and could expose sources and whistle-blowers. But you either didn't notice or care that call data retention for long periods of time, with farcical levels of oversight (in its entirety, a one-page annual document, signed by a judge), effectively constitutes mass surveillance on the entire population of Ireland, children included.''

[3] The new EU General Data Protection Directive 2016/680 and Regulation 2016/679 must be in force in Ireland by May 2018. This will necessitate a great deal of legislative reform domestically. The Directive is particularly focused on the area of crime prevention and surveillance powers. Ministry of Justice public consultations will also be forthcoming in the area.

Overview of the Issues

The core issues were summarised by Minister for Justice Fitzgerald in her statement to the Dáil in January 2016:

> 'issues of genuine concern have been raised as to the balance in our law between the important freedom of journalists to pursue legitimate matters of public interest and the basic rights of persons not to have their personal information improperly disclosed. While bodies investigating crime need to have the appropriate statutory powers available to them to carry out their duties, we need to examine the balance in respect of entirely legitimate journalistic activity being carried out in the public interest.'

It is somewhat surprising that the existence of comparatively permissive surveillance powers in Ireland came as news to the media. The Edward Snowden documents published in 2013 revealed widespread surveillance programmes being pursued by the US and UK in cooperation with Ireland,[4] and prompted a global reappraisal of how intelligence gathering is regulated. The difficult balance to be struck between effectively investigating crime in the public interest using all modern tools available, and safeguarding fundamental rights in relation to privacy, data protection, press freedoms and effective remedies (amongst other things) was brought into sharp focus. Nevertheless, as noted by the European Parliament:

> 'an analysis of Europe's surveillance programmes cannot be reduced only to the question of the proper balance between data protection and national security and to technical capabilities understood by experts. **Rather, it has to be framed in terms of collective freedoms and the nature of democratic regimes**.'[emphasis added][5]

Communications Data

The Review is focussing on various statutory bodies' access to 'communications data' retained by telecommunications service providers.[6] It is important to understand that this raw 'communications data' does not encompass content but rather constitutes 'metadata'[7] which can be described simply as 'data about data'. Whilst this term may sound relatively innocuous, metadata may incorporate important information relating to, for example: the location origins of the communication, the device used, the time the information/communication was sent, details of the recipient, information relating to the sender and recipient, the length of the communication or size of the message. Privacy International cautions that:

> 'metadata also includes data generated by our devices including: the precise location of our phone while on; where we were when our device checked for new emails; where we were when our device checked for any new social media updates, application updates or any similar automated checks.

---

[4] See, by way of example, Nicky Ryan 'Government silent as Snowden docs reveal access to Ireland's internet cables' *The Journal* 29 November 2014 www.thejournal.ie/gchq-access-to-irish-internet-cables-1806793-Nov2014/

[5] See p.18 of Didier Bigo et al (2013) 'National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law', Brussels: European Parliament Directorate-General for Internal Policies http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf .

[6] Telecommunications Service Provider' is defined at section 1 of the Communications (Retention of Data) Act 2011: 'Service provider' means a person who is engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the Internet'. Arguably, this may include a body which provides a service to persons in Ireland even where the data is either processed or stored outside Ireland. It may also include hotels, restaurants, libraries and airport lounges providing communications services.

[7] See Privacy International's website here for a detailed explanation of metadata.

> Taken alone, pieces of metadata may not seem to be of much consequence. However, technological advancements mean that metadata can be analysed, mined and combined in ways that make it incredibly revelatory. When accessed and analysed, metadata can create a comprehensive profile of a person's life – where they are at all times, with whom they talk and for how long, their interests, medical conditions, political and religious viewpoints, and shopping habits.
>
> Without appropriate protections on metadata, we can be tracked and profiled on an almost permanent and continuous basis. [...] Because of antiquated legal interpretations, metadata is ironically considered less sensitive information even though it can be used to map your life, interests, and likely future.'

The retention and disclosure of metadata clearly has widespread implications for privacy. In the context of press freedoms, any potential intrusion on journalists' private communications may inhibit sources from coming forward, and put the journalists themselves at risk especially where they are investigating issues involving serious crime including stories relating to terrorism or organised crime.[8] When considering whether specific protections may be required for journalists' over and above those for the general public's data, it is important to remember that freedom of expression under Article 10 of the European Convention on Human Rights (**'ECHR'**) entails both the individual's right to publish and read stories, but also the collective right to access an effective free press which is often seen as one of the fundamental checks and balances in a healthy democracy. Thus, any protections afforded to journalists have an indirect benefit for all. However, this is not to diminish the pressing need for the privacy rights of all to be given due consideration within this Review.

Public Interest in Effective Criminal Investigations

Suffice to say, these fundamental rights must of course be considered alongside the very legitimate public interest in public safety and an effective criminal justice system, which has the capacity to prevent and detect serious offences, and prosecute them where necessary with the benefit of the best quality of evidence obtained on a legally robust basis which cannot be subsequently challenged on appeal. Indeed, the positive obligation on public authorities to investigate crimes has been established by the European Court of Human Rights and constitutes an element of the right to an effective remedy under Article 13 ECHR and as a procedural element of the right to life, the right to freedom from torture and ill-treatment, and the right to respect for private life amongst other core civil rights.

---

[8] A good example of this arises in the case *R(Malik) v Manchester Crown Court and Greater Manchester Police* [2008] 4 *All England Law Reports* 403 in which Shiv Malik, an award-winning investigative journalist working on a book on terrorism, found himself at the sharp end of the law potentially faced with prosecution, and a wide-ranging production order forcing him to reveal his sources. The Order obtained by Greater Manchester Police under the *Terrorism Act 2000* required him to disclose ''all material in his possession'' about the terrorist activities of Hassan Butt, about another man 'A', drafts of his book and images, notes and financial information about payments to Mr. Butt and other material. The Police had also sought the journalist's ''contact lists of all persons featured in the book'', but the judge adjourned on this matter. In the judicial review, the Court approved of this incremental approach on applications for journalistic material.

Noting the inherent dilemma between public safety and press freedom, Lord Justice Dyson said: ''A balance has to be struck between the protection of confidential material of journalists and the interest of us all in facilitating effective terrorist investigations. It is for the court to strike that balance. It is for the police to satisfy the court that the balance should be struck in favour of making (the necessary) order.'' Whilst challenging police fishing expeditions, this case has had a chilling effect, as Malik was also ordered to pay the Defendants' costs despite being partly successful in his freedom of expression claims.

This has echoes of the *Mahon v Keena and Kennedy* [2009] IESC 64 case on costs in press freedom challenges, which ultimately failed in the European Court of Human Rights. See also the case of *Veronica Guerin*, which highlights the general risks of reporting on crime stories.

Section 1

Background

Public concerns were raised following reports of journalists' telephone records being accessed by the Garda Síochána Ombudsman Commission (**'GSOC'**) in the investigation of a Garda leaks inquiry. [9]

It was reported that the mobile phone records were accessed without the journalists' knowledge or consent, as part of a criminal inquiry into alleged leaks by members of An Gardaí to journalists, with information on the model Katy French who died in 2007. Media reports describe how a friend of the deceased model made complaints to GSOC about how the case was reported in the media. This lead GSOC to launch an investigation into whether members of An Garda Síochána had leaked information to journalists.[10] Two journalists' communications data was accessed by GSOC as part of this investigation.

The Minister for Justice and Equality stated that whilst bodies investigating crime need to have the statutory powers available to them to carry out their duties, there is also a need to examine the balance in respect of entirely legitimate journalistic activity being carried out in the public interest.[11] (The Minister also clarified that the Department of Justice and Equality had not authorised the tapping of journalists' phones.[12])

In the context of these developments, Fianna Fáil published a Private Members Bill to provide for the protection of journalists' sources in statute.[13] This Bill lapsed as it had not been debated upon the dissolution of the 31st Dáil. It is appended hereto as an example of the shape reforms might take.

Scope of the Review

The Review covers all bodies which may access records under the Communications (Data Retention) Act 2011 (the '**2011 Act**')[14]. Requests for data disclosure under the 2011 Act may be made by:

- A member of **An Garda Síochána** not below the rank of Chief Superintendent, where the data are required for:
  - (a) The prevention, detection, investigation or prosecution of **a serious offence**[15]
  - (b) The safeguarding of the **security of the State**
  - (c) The **saving of human life**.
- An Officer of the Permanent **Defence Force** not below the rank of Colonel where the data are required to safeguard the security of the state.

---

[9] Department of Justice and Equality (2016) 'Statement by the Minister for Justice and Equality in relation to access to telephone records' [press release] 19 January 2016, available here.

[10] See various contemporaneous media reports, including Conor Lally (2016) 'GSOC trawls journalists' phone records in inquiry' *Irish Times* 14 January 2016 and Jim Cusack and Philip Ryan (2016) ' Minister to review law allowing GSOC snoop on journalists' *Irish Independent* 17 January 2016.

[11] Department of Justice and Equality (2016) 'Statement by the Minister for Justice and Equality in relation to access to telephone records', [press release] 19 January 2016, available here.

[12] See Sarah Bardon (2016) 'Fitzgerald denies authorising tapping of journalists' phones' *Irish Times* 20 January 2016.

[13] See the Garda Síochána (Amendment) Bill 2016.

[14] Section 6 of the 2011 Act, (as amended) governs disclosure requests.

[15] Section 1 of the 2011 Act defines a 'serious offence' as one punishable by imprisonment for a term of five years or more, together with a number of Scheduled offences set out in the 2011 Act. The leaking of data by a member of An Garda Síochána is a 'serious offence' under section 62 of the *Garda Síochána Act 2005*, given the penalties attached to that offence. [The National Union of Journalists (NUJ) dispute this interpretation in their March 2016 submissions to the Review – see here] However, as a relatively minor theft offence could potentially be classed as a 'serious offence' under the Criminal Justice (Theft and Fraud Offences) Act 2001, it may be that this definition needs to be reviewed and further qualifications built into the threshold for permitting access to communications data.

- An officer of the **Revenue Commissioners** not below the rank of Principal Officer where the data are required for the prevention, detection, investigation or prosecution of a relevant revenue offence.[16]
- A Member of the **Competition and Consumer Protection Commission** where the data are required for the prevention, detection, investigation or prosecution of a relevant competition offence.[17]

Crucially in the context of the Review, the 2011 Act does not explicitly name **GSOC** as a statutory body which can access records held by telecom service providers. However, under the establishing legislation, designated officers of GSOC are conferred with the powers of An Gardaí Síochána.[18] (It excludes those Gardaí powers provided under legislation dealing with offences against the state).[19]

In this way, designated officers of GSOC can request disclosure of data from service providers, where it is required - amongst other things – for the **investigation of a serious offence**, such as the leaking of information to journalists. It is a crime for a current or former member of An Garda Síochána (or civilian staff) to disclose information, where the person disclosing it knows that it is likely to have a harmful effect.[20] The maximum penalty (where the member receives some compensation for the disclosure) is seven years' imprisonment and/or a fine of up to €75,000. This would to bring this offence into the 'serious' category.[21] (Separately to the criminal offence of leaking, the Review may wish to question whether internal disciplinary sanctions adequately reflect the seriousness of such an offence, or whether adequate civil remedies for affected third parties lie in cases of misconduct.)

The Irish Council of Civil Liberties and other groups have criticised the fact that the focus of the Review is confined to journalists' records, given that An Garda Síochána seek access to thousands of phone records annually, and that the legislation may capture a wide range of private information about members of the public.[22]

The Irish Times reported that approximately 62,000 requests for access to data were made over a five-year period, almost all by the Garda. This means that almost two requests for access are made every hour, and 34 every day. It was reported that fewer than 2% of requests for disclosure are turned down by service providers. It is difficult to verify this statistic, as one of the problems under the 2011 Act is

[16] The relevant revenue offences set out for this purpose constitute 'serious offences'.

[17] A competition offence for the purpose of data disclosure requests is defined as an offence under s.6 (2) of the Competition Act 2002, involving an agreement, decision or concerted practice. The penalties for offences under s.6 (2) are set out in s.8 of the Competition Act 2002 (as amended) and attract sentences of up to ten years' imprisonment. Again, these all constitute serious offences for the purposes of the 2011 Act.

[18] See s.98 of the Garda Síochána Act 2005.

[19] The Garda Síochána Act 2005, upon enactment, explicitly excluded the powers both under the *Offences against the State Acts 1939 to 1998*, and powers of phone tapping and surveillance under the *Postal Packets and Telecommunications Messages (Regulations) Act 1993*. However, an amendment in 2015 limited the excluded powers to those set out under the *Offences against the State Acts 1939 to 1998,* which had the effect of expanding the powers of GSOC in criminal investigations. See s.5 of the Garda Síochána (Amendment) Act 2015.

[20] See s.62 of the Garda Síochána Act 2005 which sets out a very wide set of circumstances where disclosure would be objectively considered harmful.

[21] Where the disclosure does not result in a benefit to the member, the maximum penalty is five years' imprisonment and/or a fine of €50,000, which would also satisfy the seriousness threshold. In the Parliamentary debates on the *Garda Síochána Bill 2004,* concerns were raised on the high penalties for leaking information which are imposed under s.62 of the Garda Síochána Act 2005, and noted the reliance that investigative journalists place on information from An Garda Síochána, see here.

[22] See Irish Council for Civil Liberties (2016) 'ICCL welcomes rapidity of snooping review; has 'serious misgivings' on limited scope', 19 January 2016.

that in practice the records-keeping system,[23] remedies available, and oversight around disclosure requests is scant. [24]

In terms of the scope of the Review, it is important to note that it will only focus on statutory bodies' access to 'communications data' under the 2011 Act, and not general surveillance, phone tapping, vehicle tracking or other powers which are referred to below so as to provide a complete picture within which to situate this Review.

Defining the term 'journalist'

A further interesting issue for this Review, if it is to recommend legislative change, will be how one should define 'journalists' if they are to benefit from special protection in order to protect sources. This is likely to require serious consideration in an era of 'citizen journalists' or bloggers, where anyone can set themselves up as a journalist. The dominance of internet publications written by freelance journalists, possibly based in any jurisdiction in the world, raises further regulatory challenges. The Oxford English Dictionary describes a journalist as a person employed to write for, edit, or report for a newspaper, journal or newscast, including freelancers. Journalists argue that they work pursuant to strict codes of conduct, by which they must keep confidential their sources of published materials. [25]

In contrast to other traditional professions like medicine or law, the journalist profession is largely unregulated apart from a Press Council/Ombudsman system which operates a voluntary code of practice. The NUJ does not tackle this issue head on in its March 2016 submissions to the Review. To restrict protections to those who carry membership cards for the National Union of Journalists risks discriminating against non-union members, and impacting on freedom of expression in other ways. Interestingly, the new EU General Data Protection Regulation[26] stipulates, albeit in another context, that the term 'journalist' should be interpreted widely to reflect the modern reality.

In the *Miranda*[27] case discussed below, at first instance, the High Court found that those who work alongside journalists including camera and sound assistants, editors, runners and others should also benefit from any special protection afforded to journalists. In modern journalism, there may be many others besides the writer who hold source data and this too should be born in mind in any recommendations so that they are truly effective and reflect modern press practice.

Does the nature of the story or the source's motives make a difference in any balancing exercise?

Another issue which may be relevant to the scope of this Review, if journalists' data are to be given special protection is whether, in any proportionality analysis, consideration needs to be given to the source's motives and the nature of the news story[28] where the police require access to communications data. It is instructive to compare the situation of a Garda whistle-blower with the situation arising in the Katy French case. On this issue of conscience:

---

[23] See section 9 of the 2011 Act, which sets down mandatory obligations to keep data for reporting purposes.
[24] See Conor Lally (2016) 'Give me a crash course in GSOC's Secret Access to Phone Records' *Irish Times*, 23 January 2016.
[25] There are some 30 separate systems for journalist codes of ethics in Europe. See Tiina Laitila (1995) 'Journalistic Codes of Ethics in Europe' 10(4) *European Journal of Communication* 527. We also refer to the NUJ submissions to this Review.
[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). See Article 86 and Recital 154 of the Regulation on the exemption which permits journalists to hold personal data.
[27] *Miranda v. Secretary of State for the Home Dept and Commissioner of Police of the Metropolis* [2014] EWHC 255 (Admin) and Gwendolen Morgan (2014) 'Miranda ruling conflates journalism with terrorism' *Irish Times* 1 March 2014.
[28] The discussion here on determining public interest, albeit in a different context, may be instructive - Eoin Carolan (2016) 'Establishing the public interest in media publication: the difficulties with Denis O'Brien v RTE' *Irish Jurist* 55, 189-198.

> 'the courts have traditionally regarded the source's motive in releasing information as relevant to the determination. But this is limited only to cases of wrongdoing. Thus, in *Interbrew SA v Financial Times Ltd*[29] Sedley LJ stated that if the release of information was done to expose wrongdoing, it would deserve protection, and it would not matter whether the motive was conscience or spite. If the purpose were for wrecking legitimate commercial activity, it would be less deserving of protection. Laws LJ held in *Ashworth* [discussed in the UK jurisprudence section below] that the chilling effect of court orders requiring disclosure of press sources is not lessened only because of no public interest.' [30]

Legislative Framework on Data Retention, Access and Disclosure

Surveillance powers are provided for under three main pieces of legislation in Ireland: the use of surveillance and tracking devices under the *Criminal justice (Surveillance) Act 2009* (the **'2009 Act'**); the interception of postal packets and telephone conversations (phone tapping) under the *Postal Packets and Telecommunications Messages (Regulations) Act 1993* (the **'1993 Act'**); and the use of information that has been generated by service providers arising from the use of phones and various electronic devices under the *Communications (Retention of Data) Act 2011* (the **'2011 Act'**).

By way of overview, of these forms of surveillance, only the use of 'surveillance devices' in a narrowly defined sense under s.1 of the 2009 Act requires prior judicial authorisation. The interception of the content of communications (eg phone tapping) requires only the authorisation of the Minister for Justice while the use of tracking devices and access to retained communications data takes place solely on the basis of internal approval within the Garda Síochána, Permanent Defence Force, Revenue Commissioners, Competition and Consumer Protection Commission (or, by implication, GSOC).

Under the 2011 Act, a request for disclosure of data may be made if a member of An Garda Síochána is satisfied that the data is required for the prevention, detection, investigation or prosecution of a serious offence. It is clear that the legislature made leaking of data by a member of An Garda Síochána a serious criminal offence under section 62 of the *Garda Síochána Act 2005*, thus giving power to request data in any such investigation.

As the principal piece of law at the heart of this Review is the 2011 Act, we have not gone into detail here on surveillance legislation more generally. However, the privacy and freedom of expression principles elaborated upon below, will be of relevance to this wider discussion.

Historical context

By way of background, a short description of disclosure of data legislation, more generally, is provided. This is followed by a detailed analysis of the powers conferred under the 2011 Act and a description of how the powers operate in practice.

Access to telecommunications data by An Garda Síochána and the Defence Forces was historically unregulated in Ireland.[31] Telecoms providers traditionally retained data for six years for contractual billing purposes.[32]

---

[29] [2002] EWCA Civ 274

[30] Gary Lilienthal and Ahmad (2015) 'The digital age meets the law of search and seizure: an overview of US, UK and Europe scenarios', Computer and Telecommunications Law Review 21(7), pp 219-230

[31] See TJ McIntyre (2008) 'Data Retention in Ireland: Privacy. Policy and Proportionality' 24(4) *Computer Law and Security Review* 326.

[32] Denis Kelleher (2015) *Privacy and Data Protection Law in Ireland*2nd ed. London: Bloomsbury Professional.

As noted above, the interception of post and telephone conversations ('**phone tapping**') is governed by the *Postal Packets and Telecommunications Messages (Regulations) Act 1993* (the **'1993 Act'**). GSOC were explicitly excluded from the powers prescribed under this Act, until amendments in 2015.[33] Now, GSOC can exercise powers under this legislation, subject to the same conditions applying to An Garda Síochána.

The 1993 Act established the offence of disclosing information relating to the *use* of telecommunications services. An exemption is provided where disclosures were made for the prevention or detection of crime or the security of the state.[34]

In 2002, the Data Protection Commissioner ('**DPC'**) formed the view that retention of data for six years was excessive, and instructed telecoms operators to reduce retention of data to a six-month period in line with EU law.

In the evolving context of new service providers entering the market, the Government issued a ministerial direction which required data retention for three years. When this was challenged by the DPC as an unconstitutional delegation by the Executive,[35] the Government committed to legislating for data retention in primary legislation, which eventually culminated in Part 7 of the *Criminal Justice (Terrorist Offences) Act 2005*.

Part 7 of the *Criminal Justice (Terrorist Offences) Act 2005* established a three-year retention period for telecommunications data and applied to all telecommunications providers, on foot of notice, in writing from the Garda Commissioner.

Dermot Walsh noted the manner in which this measure was introduced, as a final amendment to the *Criminal Justice (Terrorist Offences) Bill*, with a limited period for debate of the provision. Commenting on the *Criminal Justice (Terrorist Offences) Act 2005*, Walsh notes that the regime was 'not subject to the sort of independent scrutiny and review necessary to strike a reasonable balance between the right to privacy and the needs of a criminal investigation and public order maintenance'.[36] He further noted that the regime raised some very serious human rights issues, partly because the powers were framed in such broad terms and partly because of the high frequency of their use.[37] It should be noted that that legislation referred to a broader range of less serious crimes.

Walsh (2009) added that the *ex post facto* complaints procedure was of limited value when the affected person was unaware of the data access request, unless the data was then used against that person in a criminal prosecution.

Commenting on the measures introduced in the *Criminal Justice (Terrorist Offences) Act 2005*, the Data Protection Commissioner warned of the potential to 'further erode our civil liberties if they are introduced without appropriate safeguards for the privacy of law abiding citizens'. The DPC nonetheless, remained hopeful that 'through dialogue, the State can pursue its legitimate security agenda without unnecessarily and systematically intruding into each of our personal lives.'[38]

[33] See s.5 of the Garda Síochána (Amendment) Act 2015.
[34] Section 13 of the 1993 Act, amending section 98 of the Postal and Telecommunications Services Act 1983.
[35] The stated basis of the Ministerial Direction was section 110 of the *Postal and Telecommunications Services Act 1983* which confers a wide discretion on the Minister to issue directions.
[36] Walsh, D. (2009) *Human Rights and Policing in Ireland – Law, Policy and Practice* Dublin: Clarus Press
[37] Walsh, D. (2009) *Human Rights and Policing in Ireland – Law, Policy and Practice* Dublin: Clarus Press, p. 197.
[38] Annual Report of the Data Protection Commissioner, 2007.

Powers under the 2011 Act

The 2011 Act came into force on 26 January 2011. It repealed Part 7 of the *Criminal Justice (Terrorist Offences) Act 2005* (mentioned above) and amended the 1993 Act.

Amongst other purposes, according to its long title, the 2011 Act was brought into law in order to implement the Data Retention Directive 2006[39] which has since been found by the Court of Justice of European Union (**'CJEU'**) to constitute an unjust attack on the right to privacy and data protection. Despite this ruling, the Government has not amended the law and it continues to be used on a daily basis. This matter returns to the High Court in July 2016. (Please see section 2 below for further detail.)

A key objective of the 2011 Act was to oblige service providers to retain data such that relevant law enforcement agencies are empowered to make a disclosure request for that retained data. The service provider must comply with that request.[40] Importantly, content of communications is not covered in disclosure requests.

The 2011 Act was unprecedented, in requiring service providers[41] to retain data on: internet access, e-mail and internet telephony (excluding the actual content of communications). It also encompasses unsuccessful call attempts.

The retention obligation under the 2011 Act is as follows:

- **One year** in relation to internet access, e-mail and internet telephony data. [42]
- **Two years** in relation to fixed network telephony and mobile telephony data. [43]
  (Two years was the maximum retention period set out in the Data Retention Directive; the majority of EU member states opted for a shorter period).

Thus, the 2011 Act represented a reduction in the period for which telephone and mobile data is retained from three years (under the *Criminal Justice (Terrorist Offences) Act 2005*) to two years.

In each case, the data required to be retained is that which is necessary to:

- identify and trace the source of a communication
- identify the destination of a communication
- identify the date and time of the start and end of a communication (or duration of a communication for internet access)
- identify the type of communication: the telephone service used / internet service used
- identify users' communications equipment
- identify the location of mobile communication equipment (for fixed and mobile telephony)[44]

---

[39] In *Digital Rights Ireland v. Minister for Communications* C/293/12 the Court of Justice of the European Union struck down the entire Directive 2006/24/EC on the Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. (The Directive came into being as a response to 9/11 and Madrid bombings amongst others so this context is a useful reminder of its purposes.)

[40] See section7 of the 2011 Act.

[41] 'Service providers' are defined at section 1 of the 2011 Act as 'a person who is engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the Internet'.

[42] As specified in Part 2 of Schedule 2 of the 2011 Act.

[43] As specified in Part 1 of Schedule 2 of the 2011 Act.

[44] Schedule 2 of the 2011 Act.

Service providers must take measures to protect the data against accidental loss, or unauthorised or unlawful storage, processing, access or disclosure. Following elapse of the relevant retention periods, the data must be destroyed.[45] (Whether records are routinely deleted in practice is another matter, which might usefully be queried as part of the Review.)

Service providers can only access the data retained:

- At the request of the data subject
- Upon receipt of a data disclosure request from one of the state agencies (listed above)
- In accordance with a Court order or
- As may be authorised by the Data Protection Commissioner.[46]

As set out above, the state agencies entitled to make a data access request are An Garda Síochána, and by implication GSOC, the Defence Forces, the Revenue Commissioners and the Competition and Consumer Protection Commission.

Crucial to the present discussion is the fact that, in no circumstances, do state agencies ever require advance judicial authority in order to ask service providers to disclose records [i.e. no *ex ante* permission is required outside of the requesting state agency's own internal approval system.]

The data may be retained concurrently for other purposes.[47] In practice, there is no explicit ongoing requirement to analyse whether the purposes continue to be met, after the data is first obtained.

The 2011 Act requires the production of statistical reports to the Minister with supervision of the state authority, showing the number of data disclosures, on an annual basis.[48]

Complaints procedure

A complaints procedure[49] is confined to investigation of disclosures improperly made and is directed to the office of the Complaints Referee (a Circuit Court judge) set up under the 1993 Act. There is no right of appeal of a decision of the Complaints Referee, nor are written judgments published.[50]

A finding of improper disclosure, contrary to section 6 of the 2011 Act, results in a report of the findings for submission to the Taoiseach. The relevant state agency may be requested to destroy the data and there is provision for payment of compensation to the complainant. According to Digital Rights Ireland, as at September 2015, there had not been one successful complaint to the Complaints Referee.

Whilst an action for judicial review may lie before the High Court, subject to the usual rules set out in Order 84 Rules of the Superior Courts 1986, the grounds upon which such a claim can be brought are extremely narrow, rules of evidence inappropriate for this sort of challenge, and the procedure may be prohibitively expensive for the average person who suspects their personal data may have been accessed inappropriately.

[45] See section 4(1)(d) of the 2011 Act.
[46] Section 5 of the 2011 Act.
[47] Section 8 of the 2011 Act.
[48] Section 9 of the 2011 Act.
[49] See section 10 of the 2011 Act.
[50] Section 10(8) of the 2011 Act which provides that the Referee's decision is final. See also Privacy International and Digital Rights Ireland's 2015 submissions on Ireland's Privacy Record to the UN's Universal Periodic Review.

The Designated Judge

It is important to note that under the current system the designated judge is tasked only with ensuring *ex post facto* compliance with the 2011 Act by the relevant state agencies, and to report to An Taoiseach on any matters that the judge considers appropriate.[51] For the purpose of carrying out its duties, the judge has the power to investigate any case in which a disclosure request is made and may access and inspect any official documents or records relating to the request. The judge can also communicate its findings to the Data Protection Commissioner. (The current High Court judge appointed is Mr Justice Paul McDermott, whose reports from 2014 and 2015 are appended hereto.[52])

The assigned duties of the designated judge include keeping the operation of the Act under review and ensuring compliance by the state agencies with the Act's provisions. Leading privacy academic Professor TJ McIntyre has repeatedly raised concerns on the inadequacy of annual reports by the designated judge. He notes that whilst improper practices in data disclosures were identified by the Data Protection Commission, these were not raised by the designated judge. These concerns are amplified in the Digital Rights Ireland and Privacy International 2015 submissions to the UN's UPR on Ireland's human rights record.[53]

Is GSOC subject to the Designated Judge's oversight?

A question mark has been raised[54] on whether the incorporation of powers by officers of GSOC means by corollary that GSOC is amenable to oversight by the designated judge. While the powers of designated officers were carried over, it seems that GSOC is not equated under statute with An Garda Síochána. In setting out the duties of the designated judge, the 2011 Act (as amended) makes reference to whether An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Competition and Consumer Protection Commission are complying with the provisions of the 2011 Act. GSOC is not explicitly mentioned. Kilcommins and Spain (2016) note that the designated judge's report did not make reference to GSOC in the period 2011-2013. In 2014, for the first time, the judge's report refers to a visit to GSOC.

> ''The legitimate question this begs is whether GSOC was using its perceived powers under the 2011 Act prior to 2014, and, if so, what independent oversight was in place in that period. If it was using its powers under the Act between 2011 and 2014, but was not subject to oversight, does this have consequences for information gathered by GSOC during that period?''[55]

Service Providers

Memoranda of Understanding were concluded between the communications industry trade associations and representatives of the state agencies to set out guidelines on compliance with requests under the 2011 Act.[56] The Review might usefully highlight the importance of such MoUs being

[51] See section 12 of the 2011 Act. Section 8 of the 1993 Act provides that the President of the High Court, in conjunction with the Minister for Justice can invite a High Court judge to undertake the role.

[52] See Colm Keena (2016)'Phone tapping law assessments marked by brief reports' *Irish Times* 22 January 2016

[53] Privacy International and Digital Rights Ireland (2015) 'The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland, see here.

[54] See Shane Kilcommins and Eimear Spain (2016) GSOC, the Legislative Process, and the Privacy Rights of Citizens: What is the law? *Human Rights Ireland Blog* 11 March 2016.

[55] See Shane Kilcommins and Eimear Spain (2016) GSOC, the Legislative Process, and the Privacy Rights of Citizens: What is the law? *Human Rights Ireland Blog* 11 March 2016.

[56] See Ronan Lupton (2011) 'Communications Retention of Data Act 2011 (No 3)' *The Bar Review 2011,* 16(4), 85-90 (The author is a member of the Department of Justice Internet Safety Advisory Committee–ISAC and the telecommunications industry groups the Internet Service Providers Association of Ireland–ISPAI, and the Association of Licensed Telecommunications Operators–ALT O, which may be useful sources for practical information if further detail is required.)

examined by an independent body, particularly as they are not legally binding or subject to legal challenge by affected third parties. It has been reported that service providers, including Vodafone,[57] have been advised by Government not to disclose statistics of how often they are required to disclose data to statutory bodies even though the law does not prevent them from doing so.

How do the powers operate in practice?

In March 2014, the DPC issued a Report which audited An Garda Síochána by reference to the Data Protection Acts. The overall finding was of a professional police force operating in compliance with the legislation.

Of relevance for our purposes, the DPC reported on practices relating to accessing telecommunications data, primarily under provisions of the 2011 Act. During the audit, An Garda Síochána outlined that it had established a single point of contact for such requests in 2008, referred to as the Telecommunications Liaison Unit, and that requests are made via a set of designated points of contact.

An Garda Síochána described that requests for communications were made according to a set of criteria, examining:

- The legal basis for the request
- Whether An Garda Síochána could demonstrate relevance
- Whether An Garda Síochána could demonstrate necessity
- Whether the data being sought is proportionate

These criteria clearly reflect the standards developed by the European Court of Human Rights (the '**ECtHR**'), discussed below, in determining whether there has been a breach of privacy rights under Article 8 of the European Convention on Human Rights (the **'ECHR'**).

Notably, the Data Protection Acts 1988 and 2003 provide an alternative means by which agencies can access data. Restrictions on data processing do not apply where processing is required for preventing, detecting, or investigating offences etc. where the restriction would be likely to prejudice the matter.[58] However, the Report of the DPC notes that this provision is 'permissive only' in that it does not place any obligations on data controllers to provide An Garda Síochána with personal data.

In this way, the data protection legislation can be contrasted with the 2011 Act, such that the latter provides for mandatory disclosures where serious offences are concerned, whereas the former allows for 'voluntary disclosure subject to consideration on a case-by-case basis' as to whether or not prejudice might be caused.[59]

The DPC audit revealed instances of both legislative bases being cited on the making of a data request. The DPC advised that one or other statute should clearly specify the stated legal basis of a data disclosure request.

---

[57] See: Vodafone, 'Country-by-country disclosure of law enforcement assistance demands', 2015. Available at: http://www.vodafone.com/content/index/about/sustainability/law_enforcement/country_by_country.html and Jack Horgan-Jones, 'Only One Country Refused to Allow Vodafone Publish Spying data…Ireland,' TheJournal.ie, June 6, 2014. Available at: http://www.thejournal.ie/vodafone-government-refusals-makey-uppylaw-1502972-Jun2014/.

[58] This provision relates to all offences i.e. serious and non-serious offences.

[59] See Data Protection Commissioner (2014) 'Report of the Data Protection Commissioner in its audit of An Garda Síochána' pages 61-66. .

The audit examined the kind of oversight within An Garda Síochána, of the correct legal basis for a request and it was explained that 10% of all requests were reviewed as part of an internal, quarterly, audit. An Garda Síochána also explained that a number of Headquarter Directives provide instructions and guidance in relation to requests for communications data.

While the audit team was satisfied with the processes in place for internal review, it did draw attention to situations where a data request was made without the Chief Superintendent's knowledge, and authorised retrospectively, as not being in compliance with the 2011 Act. The DPC thus advised that 'all requests for call and internet traffic data should be authorised by the Chief Superintendent on a case-by-case basis rather than on an aggregate basis at the end of a particular time period'.[60] An Garda Síochána clarified that this practice had now been amended such that approval is secured in advance, and each request is considered on a case-by-case basis.

On foot of the audit, the DPC committed to issuing sectoral advice to telecommunications companies arising out of the audit.[61]

A recent example of GSOC's 2011 Act intelligence gathering powers in practice was recently aired in a Dublin District Court, in the context of a bullying and intimidation allegation made by the wife of a member of An Garda Síochána. A Garda Detective was prosecuted for giving false or misleading information to GSOC in 2012. Meteor and Vodafone records were deemed admissible in evidence. Counsel for the defence objected to disclosure of the records which it was claimed, would 'make or break' the investigation, as the only reason that they were sought was to establish whether the accused was lying.[62] The accused was found guilty and fined €500 for lying to GSOC.[63]

Communications data were also heavily relied upon by the prosecution in the *Graham Dwyer* murder trial. Such examples show the clear public interest in communications data being available, and defensible on appeal, albeit subject to the types of safeguards discussed below.

Privacy International and Digital Rights Ireland's submissions to the UN's Universal Periodic Review of Ireland provide another instructive example:

> 'Systems of internal approval are particularly open to abuse, and in 2010 a sergeant in the Garda Síochána was discovered to be using the data retention system to spy on her former partner[64]. It appears this emerged due to his suspicions and not due to any internal controls. Despite this, the sergeant in question was not prosecuted, dismissed, nor demoted, and she was transferred to a sensitive position in the Special Branch (anti-terrorist division). No details have been published as to how she was able to avoid the controls which should have prevented her abusing her access in this way, nor has the Irish State detailed any steps to review the operation of the data retention system in light of this incident.'[65]'

[60] See Data Protection Commissioner (2014) 'Report of the Data Protection Commissioner in its audit of An Garda Síochána' p.64.
[61] See the DPC's Guidance Note on Data Protection in the Electronic Communications Sector.
[62] See Andrew Phelan (2016) 'Garda and bullet sender made contact 291 timesCourt hears' *The Herald*, 20 April 2016.
[63] See Andrew Phelan (2016) 'Retired garda found guilty of lying in GSOC investigation into Valentine's Day card containing bullet and thong' *The Irish Independent* 27 April 2016.
[64] John Mooney (2011) 'Garda Who Spied on Her Boyfriend Will Keep Job' *The Sunday Times*, 14 August 2011.
[65] Privacy International and Digital Rights Ireland (2015) 'The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland, see here.

Section 2 – Balancing Competing Rights

It is clear from the earlier discussion that there is a balance to be achieved between law enforcement and national security requirements on the one hand, and privacy rights and data protection on the other.

This Section will provide an overview of the competing rights at play where data disclosure is required for intelligence gathering in the investigation of crimes. The extent to which privacy rights can be curtailed, and the potential chilling effect on freedom of expression rights and the work of journalists is outlined, with reference to Irish constitutional rights, the jurisprudence of the European Court of Human Rights ('**ECtHR'**), the requirements of EU law and the Charter of Fundamental Rights of the European Union, and international human rights standards. We provide an analysis of how comparative common law jurisdictions have addressed the balance, including the UK, US and Canada.

This section explores the kinds of safeguards which might be put in place in order to mitigate against intrusions on the various competing rights, intrusions which are sometimes necessary to achieve well-functioning law enforcement, in a democratic society.

Clear, explicit, comprehensive and transparent statutory powers together with adequately resourced judicial oversight are two means of improving the framework and these will be explored further below in Section 3 which summarises the issues which the Commission consider relevant for this Review.

Constitutional rights

The principal constitutional rights implicated in this Review (privacy and freedom of expression) are described below in summary form.[66]

Privacy

Privacy is a fundamental human right, enshrined in numerous international human rights instruments[67] to which Ireland has signed up (albeit not ones which have been incorporated domestically – but which can serve as an interpretive aid.) It is central to the protection of human dignity and forms the basis of any democratic society. Privacy rights also support and reinforce other rights, such as freedom of expression, information and association.

The Irish Constitution protects the right to privacy as an unenumerated right under Article 40.3, as established in the 1987 case of *Kennedy v Ireland*,[68] in which Hamilton P. spoke of the right 'to be let alone'.[69] This seminal case on privacy law in Ireland involved the phone-tapping of journalists, as requested by the Minister for Justice, in order to identify leaks from Cabinet. The right to privacy was not considered to be absolute, but subject to restriction, in the interests of the common good. Crucially, it was held that:

> 'The dignity and freedom of an individual in a democratic society cannot be ensured if his communications of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with […] in certain circumstances

[66] For detailed analysis see Andrea Mullan (2016) 'Constitutional aspects of international data transfer and data surveillance', *Irish Jurist* 55, 199-208.

[67] Universal Declaration of Human Rights (Article 12), International Covenant on Civil and Political Rights (Article 17); and regional standards including the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8). See also Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014.

[68] [1987] *Irish Reports* 587.

[69] Para. 592 of the judgment.

> the exigencies of the common good may require and justify such intrusion and interference.' [70]

The *Postal Packets and Telecommunications Messages (Regulations) Act 1993* (described above) was said to be a delayed reaction to the public outrage that followed this phone tapping scandal.[71]

On the other hand, in *Haughey v Moriarty*[72] the exigencies of the common good justified an interference in privacy rights (access to the Haughey family's banking records as part of the Moriarty Inquiry) as matters of public importance required an urgent inquiry.

The right to privacy has been invoked to restrain publication of details of the private life of a rape victim,[73] to protect the right to privacy of a practitioner's patients in disciplinary hearing before the Medical Council[74] and in balancing the right of a natural mother to privacy against the right of a child to know his/her natural mother's identity.[75]

A Garda leak to the media was held to interfere with the right to privacy of the subject of an imminent Garda search.[76]

The Supreme Court, in *Kane v Governor of Mountjoy Prison*[77] stated that the absence of a specific justification for the overt surveillance of an individual could constitute an infringement of privacy rights. In the particular context, justification was found in the fact that the subject of surveillance was expected to be subject to a warrant in connection with subversive activities.

Access to data on telephone usage has played a positive role in the detection and prosecution of serious crimes in Ireland.[78] In relation to the 2009 Act (described above), in *DPP v Idah*[79] the Court of Criminal Appeal said:

> 'There can be no doubt that the State may make incursions into the right of privacy in accordance with law. This is particularly the case in circumstances where the State is seeking to provide in relation to 'the investigation of arrestable offences, the prevention of suspected arrestable offences and the safeguarding of the State against subversive and terrorist threats'. Nevertheless that law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which public authorities are entitled to resort to such covert measures and it must provide necessary safeguards for the rights of individuals potentially affected. In the view of this court, that is precisely the intent and purpose of the Act of 2009.'

Privacy rights may be infringed where a legitimate public interest objective is pursued, such as the investigation of a serious crime - the more serious the intrusion, the higher the justifying threshold.

---

[70] Para. 592 of the judgment.
[71] See Maria Murphy (2013) 'The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases' Vol 3(2) *Irish Journal of Legal Studies* p. 79.
[72] [1999] 3 *Irish Reports* 1
[73] *X v Flynn*, High Court, 19 May 1994.
[74] *Barry v Medical Council* [1998] 3 *Irish Reports* 387.
[75] *O'T v B* [1998] 2 *Irish Reports* 321.
[76] *Hanahoe v Hussey* [1998] 3 *Irish Reports* 69.
[77] [1988] 1 *Irish Reports* 757.
[78] See Dermot Walsh (2009) *Human Rights and Policing in Ireland – Law, Policy and Practice* Dublin: Clarus Press, p. 197.
[79] *DPP v. Idah* [2014] IECCA 3

Where a decision affects a fundamental right such as the right to privacy (or freedom of expression) any interference with that right must be proportionate. Denham J. (as she then was) in *Meadows v. Minister for Justice, Equality and Law Reform*[80], explained this as follows:

> 'Fundamental rights arise in some cases where decisions are being judicially reviewed. When the decision being reviewed involves fundamental rights and freedoms, the reviewing court should bear in mind the principles of the Constitution of Ireland, 1937, the European Convention on Human Rights Act 2003, and the rule of law, while applying the principles of judicial review. This includes analysing the reasonableness of a decision in light of fundamental constitutional principles. Where fundamental rights and freedoms are factors in a review, they are relevant in analysing the reasonableness of a decision. This is inherent in the test of whether a decision is reasonable. And while the term 'proportionality' is relatively new in this jurisdiction, it is inherent in any analysis of the reasonableness of a decision.'

In the High Court round of *Schrems*[81], Hogan J considered that data privacy came under the protective rubric of Article 40.5 of the Constitution on the inviolability of the dwelling. He said this in the context of the US Government accessing data relating to Facebook users (albeit not specifically for criminal justice purposes, which would justify some level of interference if done lawfully):

> '51. By safeguarding the inviolability of the dwelling, Article 40.5 provides yet a further example of a *leitmotif* which suffuses the entire constitutional order, namely, that the State exists to serve the individual and society and not the other way around.
>
> 52. In this regard, it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home – such as e-mails, text messages, internet usage and telephone calls – would pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation.
>
> 53. Such a state of affairs – with its gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker - would be totally at odds with the basic premises and fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble); personal autonomy (Article 40.3.1 and Article 40.3.2); the inviolability of the dwelling (Article 40.5) and protection of family life (Article 41). As Hardiman J. observed in *The People v. O'Brien* [2012] IECCA 68, Article 40.5
>
> > '…presupposes that in a free society the dwelling is set apart as a place of repose from the cares of the world. In so doing, Article 40.5 complements and re-inforces other constitutional guarantees and values, such as assuring the dignity of the individual (as per the Preamble to the Constitution), the protection of the person (Article 40.3.2), the protection of family life (Article 41) and the education and protection of children (Article 42). Article 40.5 thereby assures the citizen that his or her privacy, person and security will be protected against all comers, save in the exceptional circumstances presupposed by the saver to this guarantee.'

[80] [2010] 2 IR 701

[81] *Schrems v Data Protection Commissioner* [2014] 6 JIC 1802

54. One might accordingly ask how the dwelling could in truth be a 'place of repose from the cares of the world' if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they could not be assured that they would not be subjected to the prospect of general or casual State surveillance of such communications on a mass and undifferentiated basis.

55. That general protection for privacy, person and security in Article 40.5 would thus be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications of this nature to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception of communications and the surveillance of individuals or groups of individuals was objectively justified in the interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards.'

Freedom of Expression

Freedom of expression is constitutionally protected under Article 40.6.1.i of the Constitution. It is a right which defends both publications made in the public interest and publications which have no public interest merit.[82]

A conflict may arise between the administration of justice on the one hand and the integrity of journalists' profession, on the other hand. A refusal to answer a question in legal proceedings has consequences for contempt of Court. In *Re Kevin O'Kelly*[83] a journalist refused to divulge details of an interview which had been recorded by him, defending his journalistic duty to foster the free exchange of ideas, and arguing that breaching the confidentiality of journalistic sources jeopardises the free exchange of ideas. Walsh J. in the Court of Appeal held that 'so far as the administration of justice is concerned, the public has a right to every man's evidence except for those persons protected by a constitutional or other established and recognised privilege'.

A seminal decision of the European Court of Human Rights ('**ECtHR'**),[84] subsequently followed by the Irish Courts, held that the protection of journalistic sources was one of the basic conditions for press freedom and that compelling disclosure of a source was contrary to Article 10 ECHR in the absence of an overriding requirement in the public interest. We have set out below a summary of the key case law from the ECtHR on the balancing exercise required when Articles 8 and 10 ECHR are in play.

In *Mahon v Keena and Kennedy*[85] the Supreme Court took account of these ECtHR principles in addressing the compulsion of journalists to answer questions posed by the Mahon Tribunal on the sources of information published in the Irish Times. The news story related to alleged payments which had been made to Bertie Ahern, and eventually led to the former Taoiseach's resignation. Fennelly J. noted the ECtHR's recognition of the value of a free press as one of the essential foundations of a democratic society, in promoting political debate, informing the public and scrutinising government. Ultimately the Supreme Court upheld the appeal from the High Court decision to require disclosure of sources. Due to the exceptional circumstances relating to the destruction of the documents, the Irish

[82] The Supreme Court held in *Mahon v Post Publications* [2007] IESC 15 that 'the media are not required to justify publication by reference to any public interest other than that of freedom of expression itself'.
[83] (1974) 108 *Irish Law Times Reports* 97.
[84] *Goodwin v United Kingdom* (1996) 22 EHRR 123.
[85] [2009] IESC 64

Times bore the costs of the proceedings. Kennedy said that: 'The principle of journalistic privilege was established but it came at such a high price that it would have a chilling effect on journalism.'[86]

The decision on costs was challenged by the journalists as, itself contravening Article 10 ECHR, but the ECtHR held by majority that the costs ruling could have 'no impact on public interest journalists who vehemently protect their sources yet recognise and respect the rule of law'.[87]

The constitutionality of the 2011 Act will be under scrutiny in the challenge by *Digital Rights Ireland v Minister for Communications & Ors*[88] which returns to the High Court for a motion hearing on 12 July 2016, with the Commission currently on record as *amicus curiae* since the IHRC joined the case in 2008.

The long-running *Digital Rights Ireland* concerns, amongst other issues, the compatibility of Directive 2006/24/EC of the European Parliament on the Retention of Communications Data, with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('**the Charter**') and Article 8 of the ECHR. The mandatory blanket retention of data by communications service providers as a surveillance measure was justified by the State on the grounds that it was a necessary and effective investigative tool for law enforcement and the protection of national security. However, the CJEU described the Directive as causing a 'wide-ranging' and 'particularly serious' interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter.

The Court found that the Directive did not include sufficient safeguards as to why and by whom such data may be accessed.[89] The Judgment noted that the Directive contained no safeguards in relation to access to the retained data, including in relation to the independence of the person authorising access to the retained data. In the long title, Ireland's 2011 Act is described as an Act to give effect to the Directive. Despite this, and in stark contrast to other member states, Ireland has not amended the legislation since the CJEU's judgment.[90]

The 2011 Act is also being challenged by Graham Dwyer, who was convicted of murder partly on the basis of communications data retained under the 2011 Act, made to enact the Directive which had been struck down by the CJEU in *Digital Rights Ireland*. His case starkly highlights the positive application of the powers, and the need for a balancing exercise to ensure law enforcement agencies are able to investigate crime effectively - albeit given the nature of the case, it is possible the Gardaí would have obtained a warrant had they had to first apply to an independent judge for permission.

[86] See Geraldine Kennedy (2014) 'A cold, calculated decision to step outside the law' *Irish Times* 25 October 2014.
[87] *Keena and Kennedy v. Ireland* (App 29804/10) Decision on admissibility 30 September 2014.
[88] Cases C-293/12 and C-594/12, 8 April 2014, at [62]
[89] In questioning the necessity of the measures mandated by the directive, the Court noted, inter alia: 'In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a Court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.'
[90] Ireland's approach contrasts with the UK which introduced the Regulation of Investigatory Powers Act 2000 Code of Practice 2015 in response together with the Data Retention and Investigatory Powers Act 2014, which has already been struck down in the High Court for falling foul of the CJEU's *Digital Rights Ireland* judgment.

International and EU developments in data retention

Edward Snowden's release of classified NSA documents on US surveillance in 2013 shifted the focus of international privacy and state surveillance globally.[91] The revelations prompted many states to re-appraise their legal frameworks and reforms have followed along with legal challenges in many jurisdictions.[92]

Reports of UN Special Rapporteurs

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, issued a report in 2013 in which he observed that:

> 'Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other'.[93]

He recommended that individuals have a right to notification of surveillance or that their communications data have been accessed by the State. Considering the need for covert surveillance, and that notification might jeopardise the effectiveness of surveillance, individuals should still be notified following the end of surveillance and be provided with the possibility of redress.

The Special Rapporteur further recommended that laws must not be used to target whistle-blowers or other individuals seeking to expose human rights violations, nor should they be used to hamper the legitimate oversight of government actions by citizens.[94]

In relation to accessing communications data, the Special Rapporteur stated that the provision of this data to the State should be sufficiently regulated to ensure that human rights are prioritised at all times and data should only be requested of corporate actors where other available less invasive techniques have been exhausted,[95] and the provision of data should be monitored by an independent authority, such as a Court or oversight mechanism.

The Report of a separate UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism produced a *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight.*[96]

Subsequently, UN General Assembly Resolution 68/167 (2014) on the Right to Privacy in the Digital Age[97] called upon states, amongst other things, to:

---

[91] See the website of the Intercept, seeking to protect transparency and accountability through journalism, here.

[92] See for example *Liberty & Others vs. Security Service, SIS, GCHQ* [2015] 3 All E.R. 212 in the Investigatory Powers Tribunal – one of a series of cases against various aspects of the UK's surveillance and the lack of oversight, which are currently going through the Courts. In the US, see *American Civil Liberties Union 'ACLU' v. Clapper* No.13-cv-03994 NY amongst other public interest claims.

[93] See para.78 of the Report of the Special Rapporteur, available here.

[94] The Report of Special Rapporteur discusses journalistic sources at length and recommends: 'National legal frameworks **must protect the confidentiality of sources of journalists** and of others who may engage in the dissemination of information of public interest. Laws guaranteeing confidentiality must reach beyond professional journalists, including those who may be performing a vital role in providing wide access to information of public interest such as bloggers, 'citizen journalists', members of non-governmental organizations, authors and academics, all of whom may conduct research and disclose information in the public interest. Protection should be based on function, not on a formal title' (emphasis added). See para.61 of the Report of the Special Rapporteur, available here.

[95] Para. 85 of the Report.

[96] A/HRC/14/46, published on 17 May 2010.

[97] See UN General Assembly Resolution 68/167 (2014) on the right to privacy in the digital age here

> 'establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data'.

EU Law

In matters within the scope of European Law, Ireland is bound by the Charter of Fundamental Rights of the European Union (the **'Charter'**) which provides for the right to respect for family life (Article 7) and the protection of personal data (Article 8). The right to an effective remedy is secured in Article 47. As with similar rights under the older European Convention on Human Rights these rights are not without qualification which protects communal interests such as public safety and crime prevention.

As noted above, in *Digital Rights Ireland* the Court of Justice of the EU (the '**CJEU**') struck down the Data Retention Directive (2006/24/EC) in light of its being a disproportionate breach of fundamental rights of privacy under the EU Charter. The Court found that the Directive did not include sufficient safeguards as to why and by whom such data may be accessed. Importantly, the Judgment did not prevent Member States implementing their own laws requiring the retention of communications data but it did critically note that the Directive itself contained no safeguards to access to the retained data, including in relation to the independence of the person authorising access to the retained data.

> 'In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.'[98][62]

A year later, Ireland was back before the CJEU. In the *Schrems v Data Protection Commissioner*[99] case, the applicant complained of the fact that Facebook Ireland Ltd transfers the personal data of its users to the US and keeps it on servers located in that country. The Advocate General stated that:

> 'Such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the Charter.'[100]

The Court agreed and also noted that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being fundamental to the rule of law. This has clear relevance for the Review where individuals have very little comeback under the current system, if they inadvertently find out that their personal communications data has been accessed unlawfully.

The EU Agency for Fundamental Rights ('**FRA'**) undertook in-depth research on the protection of fundamental rights in the context of surveillance, and published its results in 2015 (the '**FRA**

[98] See para. 62 of the judgment.
[99] Case C-362/14.
[100] CJEU C-362/14, see here for the Opinion of Advocat General Bot and see here for the judgment.

Report').[101] The focus of the study was on oversight mechanisms and remedies available. However, the FRA Report did not address the obligations of commercial entities which, willingly or not, provide intelligence services with the raw data that constitute Signals Intelligence.

Generally, it found that national legal frameworks lack clear definitions indicating the categories of persons and scope of activities that may be subject to intelligence collection. There is a vastly diverse range of intelligence systems operating across the EU.

The FRA Report identified expert oversight as being exceptionally valuable in allowing persons who are independent of political allegiances to scrutinise the actions of the intelligence services.[102] The FRA Report also emphasises the right to notification and to access information, as being crucial.

Benchmark standards of the ECtHR[103] on Privacy Rights

The case of *Klass v Germany*[104] established that privacy rights under Article 8 ECHR provide protection against surveillance by telephone tapping. However, this type of surveillance could be permissible as long as it is deemed to be: in accordance with law (which would not be satisfied by an unfettered discretion by the Executive), has a legitimate aim and is considered to be necessary in a democratic society.

The assessment against these core safeguards must be carried out in the context of the entire circumstances of the case, including: the nature, scope and duration of the measures, the authorities competent to permit, carry out and supervise such measures and the kind of remedy provided by law. In that case the ECtHR expressed a strong preference for supervisory controls to be exercised by a judge. Where any discretion is exercised in an arbitrary or discretionary manner, this will likely result in a violation of Article 8 ECHR.

Murphy[105] explains that the Article 8 phrase 'in accordance with law' encompasses a quality of law test: Legislation must comply with the rule of law, be accessible and foreseeable. The law must be sufficiently precise, and detailed safeguards developed by the ECtHR provide very specific guidance to national legislatures. There must be protection against ''arbitrary interference'' by public authorities, which takes on greater significance in cases where the government exercises powers in secret.

An interception process in the UK based on internal policy documents, and not clearly provided for in statute, was found to breach Article 8 in *Malone v United Kingdom*.[106] As noted, regulatory measures must be compatible with the rule of law, accessible and must have foreseeable consequences.[107] Foreseeability requires that citizens are given an adequate indication as to the circumstances in which, and the conditions on which, public authorities are empowered to resort to any such measures to give the individual adequate protection against arbitrary interference.[108]

---

[101] Fundamental Rights Agency (2015) *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* available here.
[102] See p. 7 of the Summary of the Report.
[103] See generally, Dermot Walsh (2009) *Human Rights and Policing in Ireland – Law, Policy and Practice* Dublin: Clarus Press, p. 164.
[104] (1979-80) 2 EHRR 214
[105] Maria Murphy (2013) 'The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases' Vol 3(2) *Irish Journal of Legal Studies.*
[106] *Malone v. UK* (1985) 17 EHRR 14 – see *Bykov v Russia* 4378/02 [2009] ECHR 441 summarising *Malone* at paragraph 78.
[107] *Liberty v UK* App. No. 58243/00 (1 July 2008).
[108] *Weber and Saravia v Germany* (App. No. 54934/00), Decision of 29 June 2006.

The right to privacy in terms of a journalists' sources attracts a higher standard of protection due to additional consequences for free expression rights under Article 10 ECHR (discussed below). The ECtHR held in *Roemen and Schmidt v Luxembourg*[109] that a search warrant will breach Article 8 if its underlying purpose was to find a journalist's sources through his lawyer.

In the case of *Marper* [110] the following core principle was set out:

> 'it is essential […] in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access to third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness'.

That case involved retention of DNA records and the ECtHR examined whether the arrangement for the storage and use of the information was sufficiently precise. Interestingly for current purposes, the ECtHR criticised the fact that DNA data was retained 'irrespective of the nature or gravity of the offence with which the individual was originally suspected', retention of data was for an indefinite period, harm suffered by minors was inadequately considered, there was no possibility for an acquitted person to have their data removed and an independent review was lacking.[111]

Recent case law post-Snowden revelations

Two helpful recent cases[112] are examined under the following headings of relevance to the Review:

- Examination of cases *in abstracto*
- Legitimate aim of protecting national security
- Foreseeability
- Effective and independent oversight, notification and effective remedies

Examination of cases in abstracto

Recent cases before the ECtHR are useful in that they challenge systems of surveillance and interception *in abstracto*, such that interferences with Article 8 rights are challenged without requiring a particular example of interception of the applicant – in other words, the applicant was not necessarily a victim of surveillance, but could have been, by virtue of the 'mere existence' of the legislation. Similarly, in the Irish High Court, Mr Schrems was found to be entitled to object to the systematic transfer of data, even if he could not easily prove that his own data would be affected.[113]

While the ECtHR does not, in general, allow for an *acto popularis* type challenge to a legislative framework and requires the existence of a specific intrusion on privacy rights, particular rules have developed in secret surveillance cases following *Klass v Germany*.[114] The unique approach in these

[109] (App. No. 51772/99), Decision of 25 February 2003.
[110] *Marper v United Kingdom* [2008] ECHR 1581.
[111] Para. 119 of the judgment.
[112] *Roman Zakharov v Russia* (App. 47143/06), Decision of 4 December 2015 and *Szabó and Vissy v Hungary* (App. 37138/14), Decision of 12 January 2016 (request for referral to the Grand Chamber pending). In the case of *Roman Zakharov v Russia* the applicant was the editor of a publishing company and promoter of free expression rights of the media. He complained that the Federal Security Service was permitted to intercept all telephone communications without prior judicial authorisation, as mobile network operators had installed equipment to enable this, pursuant to an Order of the State Committee for Communications and Information Technologies.
[113] *Schrems v Data Protection Commissioner* [2014] IEHC 310.
[114] (1979-80) 2 EHRR 214

cases is driven by a concern that surveillance measures should not become unchallengeable and outside the scope of national judicial authorities and the ECtHR.[115]

The ECtHR reiterated in *Roman Zakharov v Russia* that, in the absence of a possibility of challenge, 'widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified'.[116] In that case the ECtHR took the opportunity to clarify that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, taking into account:

- the scope of the legislation and whether the applicant can possibly be affected by it, and
- the availability of remedies at the national level.[117]

In the particular case, any user of a mobile phone was seen to be potentially affected by the legislation and in the particular case, Russian law did not provide effective remedies for a person who suspects that they have been subjected to secret surveillance. The ECtHR considered that, owing to the secret nature, broad scope and the lack of effective remedies, an examination of the legislation *in abstracto* was considered to be justified. The applicant could claim to be a victim of an ECHR violation, even in the absence of a concrete measure of surveillance.

In the case of *Szabó and Vissy v Hungary*[118], the ECtHR found a violation of Article 8, where Hungarian surveillance legislation potentially represented an unjustified and disproportionately intrusive measure, in the absence of judicial control, under sweeping anti-terrorist powers. The applicants argued that the very existence of the law permitting secret surveillance, in the absence of adequate safeguards, constituted an interference with their right to privacy.

The ECtHR held that: 'In the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance' which constitutes an 'interference by a public authority'.[119]

Legitimate aim of protecting national security

The ECtHR noted in *Szabó and Vissy v Hungary*[120] that technology had advanced since *Klass* and thus the potential interferences that accompany mass surveillance attract ECHR protections even more acutely. It noted that States have a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.

> 'In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.'[121]

An appropriate proportionality test would require supporting materials to show a sufficient factual basis for the application of secret intelligence gathering, which would enable an evaluation of the necessity of the proposed measure.[122]

[115] See *Kennedy v United Kingdom* (App. 26839/05), Decision of 18 May 2010.
[116] See para. 169 of *Roman Zakharov v Russia* (App. 47143/06), Decision of 4 December 2015.
[117] See para. 171 of *Roman Zakharov v Russia* (App. 47143/06), Decision of 4 December 2015.
[118] *Szabó and Vissy v Hungary* (App. 37138/14) Decision of 12 January 2016.
[119] See para. 53 of the judgment.
[120] (App. 37138/14), Decision of 12 January 2016.
[121] See para. 57 of the judgment.
[122] See para. 71 of (App. 37138/14), Decision of 12 January 2016.

It has been argued that national authorities should adopt decisions on proportionality *ex ante*, as *ex post* safeguards will not always be effective:

> 'First, an ex post evaluation of decisions can be complicated by the separation of powers and competences, i.e. 'who should decide whether it [proportionality] has been observed or not?' (Hoffmann 1999). The answer to this question becomes more complicated if we bear in mind that the proportionality principle does not have a normative value as such, and often national authorities have a margin of discretion in deciding. Secondly, another risk that arises in the context of an ex post evaluation of proportionality is that the balance might tilt towards allowing the taking of more intrusive measures in the face of more grave offences. We have been experiencing this especially after the September 11 events. In its evaluation, proportionality is, after all, a flexible tool that applies differently in different contexts (Jacobs 1999). Thirdly, in the presence of information asymmetry, it is difficult for national authorities to authorize the least intrusive surveillance measures available. The lack of information might be covered in those cases by the flexibility characteristic that the proportionality principle has.' [123]

This highlights the need for 'clear guidance for national authorities to aid the proper and well-informed use of the proportionality principle *ex ante*, i.e. when permitting the use of a device for surveillance purposes', such that authorities must be offered the necessary tools and information to be in a position to take proportionate decisions. [124]

Foreseeability

The law must be sufficiently detailed and precise to meet this requirement. Foreseeability takes on a special significance in the surveillance context. Citizens should not be able to predict *when* surveillance will occur (as this could defeat the purpose), but legislation 'must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures'.[125]

The ECtHR accepted that a certain flexibility is required in this regard and a detailed listing of the precise circumstances in which surveillance will occur is not required. However, discretion granted to the executive as expressed in terms of unfettered power would be contrary to the rule of law. Therefore the scope of any such discretion along with the manner of its exercise must be set out with sufficient clarity.

In the case of *Szabó and Vissy v Hungary*[126], the legislation was framed in such a way that virtually any person in Hungary could be subjected to secret surveillance. The broad-based legislative provisions enabled large-scale interception which was considered to be a matter of serious concern.

On the scope of the law the ECtHR stated in *Szabó and Vissy v Hungary* that citizens must be given adequate indication as to the circumstances in which public authorities are empowered to resort to such measures, in particular by clearly setting out the nature of the offences, with sufficient detail, which may give rise to an interception order and a definition of the categories of people liable to have their telephones tapped.[127]

---

[123] See Jonida Milaj (2015) 'Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance' *International Review of Law, Computers & Technology* p 3.
[124] *Ibid.*
[125] See para. 62 of *Szabó and Vissy v Hungary* (App. 37138/14), Decision of 12 January 2016.
[126] (App. 37138/14), Decision of 12 January 2016.
[127] Para. 243 of the judgment.

Effective and independent oversight, notification and effective remedies

In the case of *Szabó and Vissy v Hungary*[128], the surveillance measure was authorised by the Minister for Justice, which was considered by the ECtHR to constitute eminently political oversight and which did not guarantee an assessment of strict necessity, notably in the assessment of the range of persons and premises. The political nature of the authorisation also increases the risk of abusive measures.

The ECtHR has held that *ex ante* judicial authorisation is required, for example in surveillance measures targeting the media, as a *post factum* review cannot restore the confidentiality of journalistic sources once it is destroyed.[129]

The ECtHR noted in *Szabó and Vissy v Hungary*[130] and in *Roman Zakharov v Russia*[131] that the question of subsequent notification of surveillance measures is inextricably linked to the question of effective remedy, as without knowledge, an individual's recourse to challenge the justification retrospectively is limited.

Lack of notification cannot in itself lead to the conclusion that the interference is not necessary in a democratic society.

In the case of *Kennedy v United Kingdom*,[132] the lack of notification was not fatal, as any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal.[133] Ireland's lack of any such specialist tribunal or other effective remedy is likely to be deemed relevant were such a challenge to end up before the ECtHR.

In *Zakharov v Russia*,[134] unless the intercepted data was used as criminal evidence, the person would not necessarily know that their communications had been intercepted. The ECtHR noted the recommendation of the Committee of Ministers, that where data has been collected and stored without the person's knowledge, unless the data has been deleted, he or she should be informed.[135]

The ECtHR concluded:

> 'Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention.'

In a separate opinion in *Szabó and Vissy v Hungary*[136], Judge Pinto de Albuquerque held that:

> 'Mandatory third-party data retention, whereby Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law-enforcement and intelligence agency access, appears neither

[128] (App. 37138/14), Decision of 12 January 2016.
[129] See para. 101 of *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands* (App. 39315/06), Decision of 22 November 2012.
[130] (App. 37138/14), Decision of 12 January 2016.
[131] (App. 47143/06), Decision of 4 December 2015.
[132] (App. 26839/05), Decision of 18 May 2010.
[133] There have been a number of unsuccessful challenges against the adequacy of the Investigatory Powers Tribunal as a remedy for human rights breaches, as no reasons are given for decisions and no appeal lies. See *A v. B* [2009] UKSC 12
[134] (App. 47143/06), Decision of 4 December 2015.
[135] See para. 287 of the judgment.
[136] (App. 37138/14), Decision of 12 January 2016.

necessary nor proportionate. With the line between criminal justice and protection of national security blurring significantly, the sharing of data between law-enforcement agencies, intelligence bodies and other State organs risks violating the right to privacy, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. Thus, States should take steps to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy'.

Benchmark standards of the ECtHR on Press Freedom and Protection of Sources

Article 10(1) of the ECHR provides the right to freedom of expression and freedom to access and receive information (both on an individual basis, and on a collective basis of accessing information through an effective free press)[137]. Article 10 is a qualified right, subject to formalities, conditions and restrictions as set out in Article 10(2).

It is clearly established in the Strasbourg jurisprudence that a fundamental condition for the full realisation of the right of freedom of expression is that the press must be free to provide the forum in which opinions may be expressed and must be able to provide the access to information on which free expression depends:

> 'Protection of journalistic sources is one of the basic conditions for press freedom. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital 'public watchdog' role of the press may be undermined and the ability of the press to provide accurate and reliable reporting may be adversely affected.'[138]

Accordingly, the Strasbourg Court has developed, in cases such as *Telegraaf Media Nederland Landelijke Media BV v Netherlands*[139] *and Sanoma Uitgevers v Netherlands*[140], a clear position that State laws may not be used to force disclosure either of journalists' communications or the identity of their sources, save in exceptional circumstances and, even then, under strictly defined procedures of judicial oversight and approval.

The rationale for this position is that, if journalists and their sources have no expectation of the security which confidentiality affords, they may decide against providing information on sensitive matters of public interest for fear of consequences. Further, this adverse impact on the provision of information by journalistic sources will arise by virtue of the potential for identification of sources and provision to authorities of journalistic communications, even if such outcomes do not occur on every occasion that journalists are targeted by the police.

Following this line of case law, one could argue that notwithstanding the legitimate aim of investigating a 'serious office', the restriction of the right to freedom of expression in the *Katy French* case was not necessary in that alternatives might have been considered such as interviewing the journalists either as volunteers or under caution.

Impact of ECtHR jurisprudence on Irish law

[137] See generally, Dermot Walsh (2009) *Human Rights and Policing in Ireland – Law, Policy and Practice* Dublin: Clarus Press, p. 164.
[138] *Financial Times v UK* (2010) 50 EHRR 46, [59] citing the seminal case of *Goodwin v UK* [1996] 22 EHRR 123
[139] *Telegraaf Media Nederland Landelijke Media BV v Netherlands* [2012] ECHR 1965
[140] *Sanoma Uitgevers BV v Netherlands* [2010] ECHR 1284 (Grand Chamber)

Murphy[141] writes that the ECtHR has tended to focus on the 'in accordance with law' limb of the test when considering surveillance cases, as opposed to the 'necessary in a democratic society' part of the test. She argues that the ECtHR has played a key role in how surveillance law has developed in Ireland to grow into a rights-compliant surveillance regime for the interception of telecommunications. The cases of *Malone v United Kingdom,*[142] *Huvig v France*[143] and *Kruslin v France*[144] are argued to have influenced the development of the 1993 Act, resulting in a 'superficial legislative response from the Irish Government'.

Under the *European Convention on Human Rights Act 2003* public bodies must perform their duties in compliance with the Convention rights where possible, unless any statutory provision or rule of law says otherwise. Under section 4, Courts must take judicial notice of the Convention and Court's jurisprudence. Although the impact of the developing international jurisprudence on privacy rights has been limited in Ireland, this Review may be an opportunity to raise standards and bring Ireland in line with its international, EU and ECHR obligations.

Surveillance v Privacy Rights: Where does the balance lie? – Comparative Jurisprudence

Analysis of key UK cases

Interesting parallels to the circumstances giving rise to the Review arise in *News Group Newspapers Ltd v Commissioner of Police of the Metropolis*[145], more commonly known as the 'Plebgate' case, which also involved an alleged police leak to journalists, and a consequent request for disclosure which potentially placed sources at risk of being identified. The case contains a useful summary of the UK statutory framework for the acquisition and disclosure of communications data[146] and is one of the first applications of the 2015 amended Code of Practice on Acquisition and Disclosure of Communications Data[147] for police in relation to obtaining communications data involving journalists.

By way of overview, the main UK framework regulating surveillance powers, Regulation of Investigatory Powers Act 2000 (**'RIPA'**) was replaced at breakneck speed by the Data Retention and Investigatory Powers Act 2014 (**'DRIPA'**), which was then successfully challenged in the High Court on the basis of the *Digital Rights Ireland* CJEU case. The Government appealed and the Court of Appeal[148]

---

[141] Maria Murphy (2013) 'The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases' Vol 3(2) *Irish Journal of Legal Studies.*

[142] (1985) 17 EHRR 14

[143] (App. 11105/84) Decision of 24 April 1990.

[144] (App. 11801/85) Decision of 24 April 1990.

[145] [2016] 2 All ER 483

[146] 'Communications data' is defined under section 21(4) *Regulation of Investigatory Powers Act 2000* ('**RIPA**').

[147] The 2015 RIPA Code of Practice does now require a law enforcement agency seeking to obtain information about a journalist's source to apply to a judge rather than seeking an authorisation under section 22 RIPA, except in cases involving a risk to life.

[148] *Secretary of State for the Home Department v Davis* [2015] EWCA Civ 1185 (referred to CJEU in Case C/698/2015 and heard in April 2016 with judgment expected post-Brexit in late July 2016)
As above, in 2014 the Court of Justice of the European Union (CJEU) held in a case brought by Digital Rights Ireland that Directive 2006/24/EC, which obliged EU member states to require communications service providers to retain communications data for between 6 and 24 months, violated Articles 7 and 8 or the EU Charter of Fundamental Rights. It struck the Directive down. This meant that UK regulations giving effect to the Directive (the Data Retention (EU Directive) Regulations 2009) themselves became invalid. In May 2015, the Stockholm Administrative Court of Appeal referred the case of *Tele2 Sverige AB v Post- och Telestyrelsen* to the CJEU (CJEU case no C-203/15) asking the Court whether blanket data retention without any distinctions, limitations or exceptions is incompatible with the E-Privacy Directive taking account of

then referred the matter to Luxembourg and a decision is due in July 2016. Liberty, Privacy International, Justice and others have heavily criticised the new legislation going through Parliament and their legislative observations and campaigning submissions are worth considering if this Review is to make recommendations for a different regime.

In *News Group Newspapers Ltd v Commissioner of Police of the Metropolis*[149] a newspaper group and three of its journalists brought a complaint against the Commissioner under the ECHR Article 10. Communications data had been sought and obtained by the police during an investigation into an incident which took place in 2012 when the Government Chief Whip was prevented from leaving Downing Street on his bicycle through the main gate. In the context of a complaint under the ECHR Article 10 in respect of four authorisations under s.22 RIPA, the Investigatory Powers Tribunal found that one of the authorisations was neither necessary nor proportionate to the legitimate aim which it pursued and there had thus been an infringement of the complainant's Article 10 rights. The legal regime in place at the relevant time did not adequately safeguard the important public interest of the right of a journalist to protect the identity of his source. Here, by contrast to the Irish situation where there is no such statutory appeal, the journalists had a right of appeal to the Investigatory Powers Tribunal set up under RIPA 2000.[150]

The Court was influenced by the test of sufficient safeguards authoritatively laid down by Lord Bingham in *R (Gillan) v Commissioner of Police of the Metropolis* [2006] 2 AC 307 [34] as follows:

> ''The lawfulness requirement in the Convention addresses supremely important features of the rule of law. The exercise of power by public authorities, as it affects members of the public, must be governed by clear and publicly accessible rules of law. The public must not be vulnerable to interference by public officials acting on any personal whim, caprice, malice, predilection or purpose other than that for which the power was conferred. That is what, in this context, is meant by arbitrariness, which is the antithesis of legality. This is the test which any interference with or derogation from a Convention right must meet if a violation is to be avoided.''

In *R(on the application of Miranda) v Secretary of State for the Home Department* [2016] EWCA Civ 6 the Court of Appeal confirmed that the power to stop and question a person at a port or border area, and seize data including source material, under the *Terrorism Act 2000* was incompatible with ECHR Article 10 in relation to journalistic material, in that it was not subject to adequate safeguards against its arbitrary exercise. David Miranda was carrying, on behalf of a Guardian journalist, US Government material leaked by Edward Snowden when it was seized by UK police and security service using counterterrorism powers.

The Court summarised the Strasbourg jurisprudence as requiring prior, or, in an urgent case, immediate post factum, judicial oversight of interferences with Article 10 rights where journalists were required to reveal their sources (even where the source was not confidential as in that case where Snowden's involvement was a matter of public record)[151]. In concluding that the stop and search

Articles 7, 8, 15(1) of the Charter of Fundamental Rights. The Court should hand down judgment in this case, which was linked with the Liberty/Davis CJEU reference in July 2016, and its finding will be binding on all of the countries within the EU.

[149] [2016] 2 All ER 483

[150] IPT is the secretive tribunal which deals with all claims, including human rights claims, against security services and inappropriate surveillance by other bodies under RIPA 2000. It should be noted that the IPT model is no panacea of justice and is not without its critics. See *A v B* [2009] UKSC 12 and legal charity Justice's amicus brief in that challenge to the IPT's exclusive jurisdiction to hear Human Rights Act 1998 claims given the IPT's limitations in contrast to standard fair and transparent procedures when cases are heard in the normal civil or criminal courts. However, it is certainly a starting point.

[151] *Sanoma Uitgevers BV v Netherlands* [2010] ECHR 1284 (Grand Chamber) applied.

power was subject to adequate safeguards, Laws LJ in the High Court had relied on the reasoning in *Beghal v DPP* [2014] QB 607, a case which concerned Article 8 right to respect for private life. However, the Court of Appeal found that, although there was often an overlap between the two sets of rights, they were distinct, especially where Article 10 concerned freedom of journalistic expression. One of the safeguards held to be adequate in *Beghal* was the availability of judicial review. However, that was of very limited value in the context of protecting journalistic material. The availability of judicial review, after the event, could not cure a breach of Article 10 resulting from the disclosure of a confidential source or other confidential material.

The constraints on the exercise of the stop power identified by the High Court did not afford effective protection of journalists' Article 10 rights. If journalists and their sources could have no expectation of confidentiality, they might decide against providing information on sensitive matters of public interest. Therefore, the stop power was deemed to be incompatible with Article 10 in relation to journalistic material in that it was not subject to adequate safeguards against its arbitrary exercise. The natural and obvious safeguard would be prior, or immediate post factum, judicial or other independent and impartial oversight (paras 98-119)[152]. A declaration of incompatibility was made, and the law has subsequently been reviewed.

The *Miranda* case holds obvious parallels to the issues under consideration in this Review. In the *Katy French* case the offence in question, and evidence seized, had far less importance for public security than the Snowden material seized, and yet the UK Court of Appeal still saw fit to strike down the counterterrorism power – at least where journalists or their assistants[153] were concerned. Given Ireland's obligations under the ECHR and the ECHR Act 2003, it seems reasonable to assume Courts here might take a similar view on the lack of safeguards for the protection of journalists' sources and lack of effective oversight built into the legal framework.

By way of example of the UK's new RIPA 2015 Code of Practice in operation, the independent statutory Interception of Communications Commissioner's Office (**'IOCCO'**) is investigating two cases where police forces are alleged to have accessed journalists' communications data to try to identify sources. Commissioner and former Court of Appeal judge Stanley Burnton's office reported as follows:

> ''Our July 2015 report[154] sets out that we recently identified that two police forces had acquired communications data to identify the interactions between journalists and their sources without obtaining judicial approval. These breaches of the code of practice (the code) for the acquisition and disclosure of communications data were identified during IOCCO inspections.

[152] By contrast, in *Ashworth Hospital Authority v Mirror Group Newspapers* [2002] UKHL 29 a newspaper published information taken from medical records of a patient (Ian Brady) at a secure hospital and the Court found it had jurisdiction to order disclosure of source of information. However, the matter came before an independent Court and both sides had the benefit of fair procedures in determining whether the interference with their rights was proportionate. In *Ashworth,* the Lords were careful to reiterate the intention of both s10 of the Contempt of Court Act and Article 10 ECHR, their common purpose being to protect sources and that the exceptions to those two provisions must be interpreted narrowly. That said, the Court went on to consider whether disclosure would be in the interests of justice in this particular case. Acknowledging once again the chilling effect of any disclosure being ordered, the Lords felt that in this instance, disclosure was nevertheless necessary. Most important was the fact that the case concerned health data and medical records and, therefore, this had wider implications -- such data should be safeguarded in any democratic society. They were also concerned to point out that the disclosure had been made worse because it was purchased by a cash payment.

[154] See paras 3.10-3.26 of the IOCCO's July 2015 statutory half yearly report http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf

> We made clear in our half-yearly report that we were in the early stages of investigating these breaches and determining whether any individual has been adversely affected by any wilful or reckless failure by any person within a public authority. If we establish that fact we will, in line with paragraph 8.3 of the code, inform the affected individuals of the existence of the Investigatory Powers Tribunal (IPT) and its role to enable them to engage the IPT effectively.''

We have already highlighted the fact that – although outside the scope of the Review's Terms of Reference - ordinary citizens, adults and children, are equally at risk of having their communications data seized when the criteria under the 2011 Act are met. In *Miranda*, the Court reasoned that journalists should be afforded greater protection as the breach of their freedom of expression rights was immediate, and judicial review after the fact to challenge a breach would not amount to an effective remedy – the source's identity would have been revealed and systemically there would be a 'chill effect' on freedom of the press generally. By contrast, privacy rights could be vindicated by a retrospective Court challenge. This is an issue which the Review may wish to consider more carefully.

Canada and US jurisprudence

Beyond Europe, Courts in Canada and the United States have recently issued decisions affirming that surveillance measures, including mere access to data retained by communications service providers, must be subject to judicial control or dependent upon the issuance of a judicial warrant.

In the case of *R v Spencer*[155]*,* the Supreme Court of Canada considered whether police obtaining identity information from an Internet Service Provider ('**ISP**') without prior judicial authorisation, which information was subsequently used to convict an accused of possession of child pornography, was in compliance with the Canadian Charter of Rights. The Court considered that a request from police that an ISP voluntarily disclose identity information amounts to a search. Given that *'[a] warrantless search, such as the one that occurred in this case, is presumptively unreasonable'* the Crown had to rebut the presumption by establishing that the search was authorised by law, and carried out in a reasonable manner. The Court found that there was no lawful authority for the police's search, and thus it was unlawful.

The US case of *Riley v California*[156] concerned the search of digital information on a cell phone. The US Supreme Court considered whether police were required by the Fourth Amendment to the US Constitution, which pertains to search and seizure, to obtain a judicial warrant prior to conducting such a search. In a unanimous decision, the Court held that the police generally may not search digital information on a cell phone seized from an individual who has been arrested without first obtaining a judicial warrant.

The Supreme Court began by noting the general principle in US law that surveillance should be subject to judicial control:

> ''As the text [of the Fourth Amendment] makes clear, 'the ultimate touchstone of the Fourth Amendment is 'reasonableness.'' Our cases have determined that '[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, … reasonableness generally requires the obtaining of a judicial warrant.' Such a warrant ensures that the inferences to support a search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.' In the absence of a warrant a search is reasonable only if it falls within a specific exception to the warrant requirement.''

[155] *R v Spencer* 2014 SCCC 43, at [68]
[156] *Riley v California* 573 U.S. 5 (2014), p. 5

The Court went on to consider, at length, the application of such principles to the unique situation of post-arrest mobile phone searches. It concluded its opinion with a reminder that the principle of judicial control of surveillance measures was one of the driving forces behind the American Revolution:

> ''Our cases have recognised that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that '[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance.' According to Adams, Otis's speech was 'the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child of Independence was born.'
>
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. **Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple – get a warrant.'' [p28]**

A recent decision of the 11th Circuit Appeals Court[157] established that police must obtain a judicial warrant prior to obtaining mobile phone location data from communications services providers. The Court found:

> ''While committing a crime is certainly not within a legitimate expectation of privacy, if the cell site location data could place him near those scenes, it could place him near any other scene. There is a reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute. Again, we do not see the factual distinction as taking Davis's location outside his expectation of privacy. That information obtained by an invasion of privacy may not be entirely precise does not change the calculus as to whether obtaining it was in fact an invasion of privacy [...] The obtaining of that data without a warrant is a Fourth Amendment violation.''

As set out in the Section 1 discussion on 'communications data' or 'metadata' above, metadata embraces the 'who', 'when' and 'where' of a communication but not the content. However, it enables automated location and relationship inferences, is densely interconnected, can trivially be re-identified, and can be used to determine highly sensitive traits.[158] The issue is neatly encapsulated in the case of *Klayman v. Obama*[159], in which a federal court judge invalidated a central NSA program, noting that metadata from each person's phone 'reflects a wealth of detail about her familial, political, professional, religious, and sexual associations' [160]. Ireland could be at the vanguard in terms of moving the law on from the analogue to the digital era if these features of metadata were to be reflected in any new framework proposed.

---

[157] *United States v. Davis*, 2014 U.S. App. LEXIS 10854 (11th Cir. June 11, 2014)

[158] Mayer et al (2016) 'Evaluating the Privacy Properties of Telephone Metadata' Vol 113(20) *Proceedings of the National Academy of Sciences.*

[159] *Klayman v. Obama* 957 F. Supp. 2d 1, Dist. Ct. DC (December 16, 2013)

[160] See contrasting comments in *ACLU v. Clapper*, No. 13-cv-03994, Southern Dist. Ct. NY (August 26, 2013) and *ACLU v. Clapper*, 959 F. Supp. 2d 724, Southern Dist. Ct. NY (December 27, 2013)

Standards developed by civil society

Whilst not legally binding, the following standards are worth referring to for guidance and, in particular, the first set of principles, which is set out in full in Appendix C.

- *International Principles on the Application of Human Rights to Communications Surveillance* - endorsed by almost 400 non-governmental and human rights organisations, May 2014.
- *Global Principles on National Security and the Right to Information* (Tshwane Principles) Open Society Justice Initiative, 12 June 2013, drafted by 22 organisations and academic centres[161]
- *Johannesburg Principles on National Security, Freedom of Expression and Access to Information* adopted by a group of experts convened by Article 19 in 1995[162]
- *Principles of Oversight and Accountability for Security Services in a Constitutional Democracy*, 1997, Centre for National Security Studies (CNSS) and the Polish Helsinki Foundation for Human Rights.[163]
- Big Brother Watch 2015 Recommendations on reform to RIPA[164] and the Interception of Communications Commissioner's Office (IOCCO)'s 2015 statutory oversight report.

[161] See https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf
[162] See https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf
[163] See http://www.right2info.org/resources/publications/national-security-page/principles-of-oversight-and-accountability
[164] See https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/05/Big-Brother-Watch-Report-Police-Communications-Data1.pdf

Section 3

Overview of Human Rights Issues

The Commission considers that the inadequacy of checks and balances on the use of the powers under review is a cause for great concern from a human rights perspective. In light of the international standards emerging on data privacy and crime prevention, and the importance of press freedom both as an individual and collective right, the issues arising in the context of this Review include the matters summarised below. Should you wish to discuss any of these issues in further detail, please let us know.

The issues for consideration are grouped broadly under three headings:

1. Rationale for reform
2. Quality of law, and
3. Implementation in practice.

1. Rationale for reform

In contemplating any reform, it is useful to consider the wider benefits of protecting privacy rights, which are inextricably linked to the protection of free speech, free association, the right to protest, freedom of conscience, and trust in government, amongst other side benefits to the public.

In addition**,** more legally robust systems bolster the appropriate use of communications data evidence in criminal trials and serve to avoid trials collapsing, or appeals arising as in the *Dwyer* case. Victims benefit. Equally, systems with stronger safeguards mitigate the risk of miscarriages of justice arising.

The implications of reforming the law in relation to 'metadata', as distinct from content data, should be explored. Questions surrounding the kind of personal information which metadata can disclose and whether a higher standard of protection is warranted for contents data (in the modern era of data analytics) deserve some attention. In broaching this distinction, Ireland could be at the forefront in designing legislation which reflects the modern reality of metadata.

It is clear from the legal framework set out above, that there is impetus for improving the current legislation if one follows Irish constitutional law, EU, ECtHR and international human rights standards. This is especially so in relation to the lack of special safeguards for the communications data of journalists (or other professionals with duties of confidentiality including religious ministers, doctors, members of Parliament and lawyers – albeit falling outside the narrow Terms of the Review).

Parallel developments to transpose the EU General Data Protection Directive 2016 by May 2018 into Irish law, will result in privacy rights and the DPC's role being bolstered. Alongside the forthcoming *Digital Rights Ireland* case challenging the 2011 Act head-on, this offers a unique opportunity to consider wider reforms to surveillance law.

As Oireachtas Committees are currently being re-established, a joint parliamentary committee on surveillance, with access to IT and human rights expertise and resources, may also be considered.

2. Quality of law

As set out in Section 2, the legality principle requires that intrusions on privacy rights are 'in accordance with law'. This encompasses a 'quality of law' standard, and requires that the law be accessible, foreseeable and must ensure that surveillance measures are only applied when necessary in a democratic society. The law must provide for adequate and effective safeguards and guarantees against abuse. Applying a proportionality test within the legal framework and in individual access

requests is one of the most effective ways of ensuring the balancing exercise is conducted as a matter of course. Such an approach also has the benefit of providing the State with an opportunity to formally legitimise any necessary interference with privacy rights.[165]

The law should be accessible and foreseeable

The law should be sufficiently clear and transparent to ensure that it is both accessible and that individuals can foresee the circumstances in which the power may be used. Importantly, this does not mean always being advised in advance that one's data is about to be accessed as this could defeat the purpose; rather it means that the rules of the system are clear to all.

However, the possibility of affected individuals being notified in certain cases, should be considered as a means of improving transparency. For example, where a case has been closed, line of inquiry abandoned, or case of mistaken identity realised, the statutory agency could write to let an individual know their data was lawfully accessed under the 2011 Act but has now been safely deleted. Alternatively, as a less onerous step to automatically informing those whose data was accessed, the statutory agency could at least reply to a specific request from an affected individual to confirm the breach and provide brief ECHR and *Mallak*-compliant reasons[166] for the data access. This would go some way to improving on the current culture where no meaningful response is often provided in light of perceived 'tradecraft' or confidentiality requirements.

This issue in turn links to the right to effective remedies where fundamental rights have been breached. Although this would only be in rare circumstances, it is important to have systems in place to guard against arbitrary use of the powers, and provide adequate redress where there have been breaches. As set out above (Section 1) the current complaints mechanism does not appear to provide an effective remedy and is not open to appeal. The complainant is limited to arguing that a disclosure request was improperly made. Such a proven contravention does not in itself render the disclosure request invalid. Nor is there any independent tribunal route open to individuals who inadvertently learn that their data has been accessed inappropriately. Whilst judicial review proceedings provide an avenue to challenge powers improperly exercised by public bodies, grounds and remedies are extremely limited, and normal rules of evidence not appropriate for many cases. Equally, own litigation costs and the risk of adverse costs, delays and publicity may deter many affected persons.

Under the 2011 Act, there is no obligation on the relevant bodies to keep a record of the reasons for requesting access to the data. The obligation to carefully document and justify intrusions on privacy rights would serve to create a culture of accountability. The default presumption should be that such documents would be subject to disclosure in litigation. This in turn could lead to greater accountability.

Related to the legality principle is the fact that powers are only conferred on GSOC by implication. They are not clearly named in the 2011 Act. The Commission nevertheless notes, and had previously observed, that given GSOC's vital role as a watchdog, there is a need for it to have effective powers of investigation.

Necessary in a democratic society, and in each individual case

The definition of 'serious offence' is potentially extremely wide and the Review may wish to query whether, given the fundamental rights engaged, further qualifications should be built into a statutory threshold test. This would avoid the current situation where, for

[165] See Jonida Milaj (2015) 'Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance' *International Review of Law, Computers & Technology* p 3.
[166] *Mallak v. Minister for Justice, Law Reform and Equality* [2012] IESC 59

example, the mere anticipation of a relatively minor theft offence comes under the definition of 'serious offence', thereby permitting full access to a person's intimate communications data.

The 2011 Act requires a blanket retention policy by service providers for two years, without distinction as to the usefulness of the material being retained i.e. it is not limited to what is strictly necessary.

Then, in the 62,000 cases over 5 years in which a request for data is made by one of authorised statutory bodies, the standard of evidence required before a request can be made seems to be *de minimis*. Privacy rights of persons who have not committed any offence are compromised (e.g. journalists, witnesses, a victim's family members, friends or neighbours). What are the implications of widespread data disclosure requests, and possible 'fishing expeditions' in relation to innocent parties? Should the level of suspicion required for a person to be connected to a serious offence be defined?

As below, statutory agencies should have to document what less invasive investigative techniques were first considered so as to ensure that access to communications data is not used by default, but only as a last resort 'where strictly necessary in a democratic society,' as required by Article 8 ECHR.

The Commission considers there is potential to boost An Garda Síochána's existing practices, as set out in the DPC report (see Section 1), and extend good practice to the other statutory bodies, whose internal systems have been less under scrutiny to date. The Review may also wish to suggest that, in the interests of transparency, any such Gardaí Directives or guidance be placed in the public domain.

Proportionality test required – both in the legal framework and in individual data requests

As above, the current legislation has no in-built proportionality test. While we noted in Section 1 that An Garda Síochána incorporates a basic proportionality test in its internal assessment criteria, the inclusion of an explicit and more detailed proportionality clause in primary legislation, or a statutory code of practice, would serve to enhance checks and balances, and to ensure consistent application by all statutory bodies with disclosure request powers.

A lawful proportionality assessment involves balancing the seriousness of the interference against the need to investigate a serious crime. An authorisation to invade an individual's private life must have a clear consequential benefit to the investigation, must not be disproportionate, or arbitrary. An interference is not considered to be proportionate, if the end could have been achieved by less intrusive means.

The following elements of proportionality should therefore be considered, and documented:

- Balancing the size and scope of the proposed interference against what is sought to be achieved;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the data access request is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the communications data sought.

Where there is a risk of journalist's source data being identified, a proportionality analysis of the risks of interference with Article 10 ECHR on press freedoms would need to be carried out, and ideally the law enforcement body would make an advance application to a judge *in camera* except in urgent

cases. (By way of example of how this works in practice, see the UK's 2015 Code of Practice in relation to Communications Data,[167] which is discussed in Section 2 above in more detail. The US and Australia operate similar models requiring prior judicial authority before journalists' communications data are interfered with, given the attendant risk to the communal interest in an effective free press.) If the Review is to make a special case for journalists, we refer to the section on defining journalists above.

Adequate and effective safeguards

Overall, there is a need for safeguards in relation to the procedural as well as substantive aspects of the fundamental rights in play.

The Review may wish to question whether a law which provides that anyone's metadata might be accessed without notification, with very limited transparency and with inadequate foreseeability as to whose data might be accessed, provides sufficient safeguards for the fundamental rights engaged.

As noted above, arbitrariness is antithetical to the legality principle, and the rule of law more generally. The 2011 Act does not adequately guard against arbitrariness and the consequent risk of abuse. The example of a Garda member reportedly using surveillance powers to stalk an ex-partner, and incurring only a minor sanction, raises serious questions over whether the safeguards are adequate. The Commission considers that the current system should be amended so that any unlawful or abusive use of data accessing powers is subject to proportionate internal disciplinary action, and criminal sanctions which reflect the seriousness of the abuse of power. Guideline minimum penalties could be considered.

Independent oversight is an important safeguard against abuse. Currently, oversight appears to be limited to a regrettably brief annual post facto review by a busy High Court judge in their spare time. While the power to review the operation of the law (as set out in the 2011 Act) has some potential for a rigorous assessment, the reports of the designated Judge have to date failed to exploit the full potential of an operational review. An effective independent oversight body could have power to refer to an independent tribunal which could provide an effective remedy, and full provision for reporting of errors with mandatory consequences for data controllers in case of breaches e.g. inspections, reporting requirements, supervision orders.

Clearly, such a system also needs to be balanced against the need for efficient crime investigation system not overly hampered by regulatory requirements. What the Commission is suggesting is a core irreducible minimum which will serve to bolster the system overall, and restore public confidence.

3. Implementation in practice

The powers appears to be in widespread use with almost 2 requests for access to data per hour (62,000 in 5 years), mainly by An Garda Síochána and fewer than 2% of these are declined. More rigorous statistics need to be maintained in strict adherence with the requirements under section 9 of the 2011 Act.

In defining the 'designated' person entitled to approve requests from rank and file officers, the Review may wish to make some practical suggestions to enhance safeguards against abuse. To build independence guarantees into the current system, one could mandate that the decision-maker be

[167] See paragraphs 3.73-3.84 in relation to journalists, members of Parliament, religious ministers and medics: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

independent from operations and investigations, and build in a randomised component to ensure this. Mandatory training in human rights and equality, and access to expert assistance would also help.

Further questions for the Review include the following: once data is accessed, how is it stored by the An Garda Síochána, GSOC, Revenue, Defence Forces, Competition and Consumer Commission or any other body concerned? Is it secure? Is it deleted after 2 years as required by law for service providers? What about restored data? What safeguards are in place to prevent widespread access or sharing with other agencies? Given the data can then be held concurrently for other purposes, where are those purposes recorded? Should it be reviewed periodically to ensure legitimate purposes are still satisfied in each case?

The role of private actors in large-scale data collection may need to be explored further by an independent body, along with the practice of non-legally binding MoUs being drawn up with telecommunications service providers.

Any new system of oversight should be adequately resourced in terms of parliamentary time for regular review of legislation, record-keeping by those empowered to access data, and should have full access to technical systems with access to IT, academic and privacy experts for inspections. It is clear that under the current system neither the Complaints Referee nor Designated Judge have adequate time nor recompense nor technical expertise to allow them to do their job effectively.

Any oversight mechanisms should be public-facing and staff should have access to regular training.

Having such safeguards in place would hopefully go a long way to restoring public confidence in law enforcement systems, and enable the system to work more effectively and transparently in everyone's interests.

Previous Statement of the Former IHRC on surveillance and privacy

Although the 2009 legislation is outside the scope of this Review, it is worth considering the former IHRC's legislative observations on the *Criminal Justice (Surveillance) Bill 2009*. It welcomed the safeguards included in that framework, including the judicial supervision of an authorisation for surveillance, in most circumstances. The former IHRC also welcomed the fact that the officer, superior officer or District Court judge, as the case may be, must be satisfied that surveillance is the least intrusive means available, that the surveillance is proportionate to its objectives having regard to the likely impact on the rights of person and that the duration of surveillance is reasonably required to achieve its objectives.

The former IHRC, nonetheless, raised a number of issues with the legislation. Having set out the principles of privacy rights (pertaining at that time), it raised concerns on the lack of safeguards surrounding the use of CCTV cameras for the investigation and detection of offences. With regard to tracking devices, the former IHRC recommended that there should be judicial supervision of the use of such devices. Recommendations were also made regarding enhancement of effective remedies under the legislation such that a person who has been subject to surveillance, can exercise their right to a remedy. It was further recommended that relevant state agencies should regularly furnish information to the designated judge. The consequences of a material contravention of the legislation were also explored, in terms of the possibility of further investigation.

Interestingly, for the present purposes, the former IHRC addressed the omission of GSOC as a relevant agency under the legislation, such that GSOC would not be conferred with surveillance powers. The former IHRC noted that:

> ‘‘A failure to extend surveillance powers to the body which is charged by the Oireachtas with independent oversight of the police may seriously limit the capacity of GSOC to discharge its functions effectively as they relate to the investigation of arrestable offences.’’

It observed that the failure to extend the power to GSOC may undermine confidence in the body to effectively investigate serious wrong-doing. Finally, the former IHRC recommended that emerging codes of practice be proofed against underpinning human rights standards.

APPENDIX A

International Principles on the Application of Human Rights to Communications Surveillance - endorsed by almost 400 non-governmental and human rights organisations, May 2014.

The Principles

Legality

Any limitation imposed on an International Human Rights must be prescribed by law. Sufficient notice should be given if a proposed law is going to limit one of these rights. The law should be clear, and given periodic review to ensure it remains effective given the speed of technological development.

Legitimate Aim

Communications surveillance should only be used by permitted state authorities where necessary in a democratic society. Any situation where discrimination arises should not be used.

Necessity

Surveillance laws should be limited to those which are necessary to achieve a legitimate aim, or where there are multiple means but Communications Surveillance is the least intrusive method on International Human Rights. The onus of establishing necessity should remain with the state[23]

Adequacy

Any communications surveillance authorized by law must be appropriate for the legitimate aim it is fulfilling.

Proportionality

Communications Surveillance is regarded as a highly intrusive act, and therefore must consider the sensitivity and severity of the situation. The state should establish the following prior to conducting communications surveillance:

- There is a high chance of serious crime or specific threat
- There is a high degree of probability that relevant evidence will be obtained.
- Other less invasive techniques have been exhausted, such that communications surveillance is the least intrusive method
- Information collected will be confined to only which is relevant
- Excess information obtained will be returned or destroyed
- The information accesses will be used by the specific authority for the purpose the authority was given
- The requested authority to use communications surveillance does not undermine the purpose of the right to privacy or other fundamental freedoms.

Competent Judicial Authority

The authority determining the validity of the communications surveillance must be independent of those conducting the surveillance, and be competent when making these decisions.

Due Process

That everyone is entitled to a fair and public hearing within a reasonable time by a competent judicial authority. Due process can be used interchangeably with 'procedural fairness' and 'natural justice'[24][25]

User Notification

Those subjects of Communication Surveillance should be given the opportunity to challenge the decision when a decision authorizing Surveillance has been issued. The materials presented in support of the application should be available for those subjects. Delay in notification is acceptable where notification would frustrate the purpose of communication surveillance and authorization is granted by a competent judicial authority.

Transparency

Information about use and amount of Communication Surveillance should be available to those who request it. States should provide the requestor with information sufficient to ascertain the nature of the request and determine the size of both the request and those who will be affected by it. Records of requests for communications surveyed should also be published.

Public Oversight

States should establish an independent position to oversee the use of Communications Surveillance and to ensure transparency and accountability. The person(s) in this position would have sufficient authority to access all potentially relevant information, to assess whether the State is making legitimate use of its lawful capabilities, to evaluate whether the State has met its transparency obligations, and to make public determinations as to the lawfulness of those actions. The document in this instance makes reference to the United Kingdom's Interception of Communications Commissioner as an example of such an independent oversight mechanism.[26]

Integrity of communication and systems

States should not require those service providers or software/hardware vendors to build surveillance/monitoring capability into their systems. People have a right to express themselves anonymously.[27]

Safeguards for International Cooperation

Where a state has entered into a mutual legal assistance treaty(MLAT) or other multi-jurisdictional agreement where more than one legal jurisdiction overlaps, the laws that apply are those which have the higher level of protection for the individual. MLAT's should also be transparent, publicly available and subject to guarantees of procedural fairness

Safeguards against illegitimate access and right to effective remedy

Communications surveillance by third parties should be prohibited with sufficient penalties. Protection for whistle-blowers should be enacted. Any information obtained by means not consistent with these principles should be inadmissible as evidence. Once information collected by communications surveillance has been used for the purpose for which it was collected it should be promptly destroyed or returned.

APPENDIX B

Garda Síochána (Amendment) Bill 2016: First Stage

Deputy Niall Collins: I move: That leave be granted to introduce a Bill entitled an Act to provide for the protection of journalists' sources.

This Bill, which was drafted by the Fianna Fáil party and submitted in my name, arises from issues which arose in the public media in the past two or three weeks regarding access to phone records of certain members of the journalistic community. It is important to point out that none of us is above the law, and this includes journalists. At the same time, it is of paramount importance that the independence and freedom of the press are respected and upheld.

The issue that came to fore, and that was brought to our attention, was the fact that the test that GSOC applied on whether to access the records of journalists - and, by extension, people with whom they had been in contact - was not clear. There is no transparency around it; nor is there an appeals process or oversight mechanism. To assuage these fears and concerns, and to protect the independence and freedom of the press and the independence of GSOC, we have drafted and tabled this Bill, which provides for judicial oversight of GSOC when it seeks to access the phone records of a journalist or broadcasting organisation. It allows the parties having their records accessed to make a submission to the High Court as part of the oversight process. GSOC would apply to the High Court for an authorisation to access phone records, and the journalist would have the opportunity to make a submission or objection as part of the process. The Bill has a double benefit in that it provides an opportunity for journalists to have their say, to protect their sources and to uphold their independence and the freedom of the press, while at the same time bolstering the independence of GSOC, which has a very important job to do and is charged under various legislation, primarily the Garda Síochána Act 2005, with doing a very important job on behalf of the citizens of the country.

An Ceann Comhairle: Is the Bill opposed?

The Taoiseach: No.
Question put and agreed to.

An Ceann Comhairle: Since this is a Private Members' Bill, Second Stage must, under Standing Orders, be taken in Private Members' time.

Deputy Niall Collins: I move: 'That the Bill be taken in Private Members' time.'
Question put and agreed to.

APPENDIX C Designated Judge's reports of 2014 and 2015

Report of the Designated Judge Pursuant to Section 8(2) of the Interception of Postal Packets and Telecommunication Messages (Regulation) Act 1993 and Section 12(1)(c) of the Communications (Retention of Data) Act 2011

I am the "Designated Judge" under the above mentioned Acts.

On 24th October, 2014, I attended at the Headquarters of An Garda Síochána at "the Depot", Phoenix Park, Dublin and later in the afternoon of the same day, at the Headquarters of the Army in McKee Barracks, Blackhorse Avenue, Dublin.

On 31st October, 2013, I attended at the Office of An Garda Síochána Ombudsman Commission, 150 Upper Abbey Street, Dublin and later on the afternoon of the same date at the Office of the Revenue Commissioners, Block D, Ashtown Gate, Dublin 15.

On the morning of 6th November, 2014, I attended at the Office of the Department of Justice and Equality, St. Stephen's Green, Dublin 2.

In each of these locations, such documents and records pertaining to the operation of the above Acts as were requested by me, were made available and were examined by me. I also spoke with the persons with responsibility for and overseeing the operation of the above Acts, in each location and all of my queries were answered to my satisfaction.

I am satisfied that as of the date of this report, the relevant State authorities are in compliance with the provisions of the above Acts.

Mr. Justice Paul McDermott
13th November, 2014

REPORT OF THE DESIGNATED JUDGE PURSUANT TO SECTION 8 (2) OF THE INTERCEPTION OF POSTAL PACKETS AND TELECOMMUNICATIONS MESSAGES (REGULATION) ACT 1993 AND SECTION 12 (1) (C) OF THE COMMUNICATIONS (RETENTION OF DATA) ACT 2011

1. As the "Designated Judge" under the above mentioned Acts I arranged to visit the relevant authorities to examine files and records concerning the operation of the powers vested in them under the above Acts. On 23rd October 2011 I attended at the Office of the Department of Justice and Equality, St. Stephens Green, Dublin 2 and met with officials who made available to me documents and records relating to the operation of the Acts, as requested. I examined the files and records furnished and spoke to the officials responsible for the operation of the Acts and liaison with other authorities in respect of same. All documents requested by me were furnished and all questions posed by me in relation to the files and records produced were answered to my satisfaction.

2. On 30th October 2015 I attended at the Office of the Revenue Commissioners at Block D, Ashtown Gate, Dublin 15 and the Headquarters of the Defence Forces at McKee Barracks, Blackhorse Avenue, Dublin. In each of these locations such documents and records relating to the operation of the above Acts as were requested by me were made available to and examined by me. I spoke to the officers and personnel responsible for the operation of the above Acts at these locations. I had a number of questions in relation to the files produced which were answered to my satisfaction.

3. On the afternoon of 30th October 2015 I attended at the headquarters of An Garda Síochána at "the Depot" Phoenix Park, Dublin where I met with officers and personnel responsible for the operation of the above Acts. I examined computer

records and hard copy files relating to the operation of the above Acts which were made available for my inspection and all documents and records which I requested were furnished and examined. All questions posed by me in relation to the operation of the Acts and the documents and records produced were answered to my satisfaction.

4. On 3rd November 2015 I attended at the offices of An Garda Síochána Ombudsman Commission at 150 Upper Abbey Street, Dublin 1 and there met with members of the Commission and personnel responsible for the operation of the above Acts. All documents relevant to the operation of these Acts which I requested were furnished and questions posed by me were answered to my satisfaction.

5. I am satisfied having examined the records and documents produced to me and from the information conveyed to me at these meetings that the relevant State authorities are in compliance with the provisions of the above Acts as of the date of this report.

Mr. Justice Paul McDermott
6th November, 2015