Review of the Law

on the

Retention of and Access to Communications Data

Mr. Justice John L. Murray

April 2017

TABLE OF CONTENTS

Acknowledgments

This report entailed a review of legislation. It was not an investigation of any events or operations and had no statutory powers of investigation or compulsion. I am very grateful, therefore, to all those who voluntarily assisted the Review in understanding the practical realities of the complex intersection between modern communications networks and their use by the public and journalists and the law on the retention of data.

A special acknowledgement to Mr. Andrew Munro of the Department of Justice and Equality who was part-time Secretary to the Review, for his excellent advice and contribution to its work from the outset to its conclusion.

A particular debt of gratitude is owed to Professor Finbarr McAuley, a former member of the Law Reform Commission and Emeritus Professor at the Sutherland School of Law, UCD for his very many invaluable hours of work in reading and editing the draft report. Once again, his commitment to the public interest is evidenced by the fact that he has carried out this work on a voluntary basis.

All of the judges and statutory bodies with powers and obligations under the 2011 Act were extremely cooperative.

I would like to thank the Hon. Mr. Justice Paul McDermott of the High Court for his insight into the role of the "designated judge" for the purposes of section 12 of the Communications (Retention of Data) Act 2011, and His Honour Judge John Hannan of the Circuit Court for his assistance in understanding the functions of the "Complaints Referee" for the purposes of section 10 of the Communications (Retention of Data) Act 2011.

Considerable gratitude is also due to: the Garda Commissioner, Ms. Nóirín O'Sullivan and all the members of the Garda Síochána who assisted the Review, particularly Chief Superintendent Peter Kirwan and his colleagues; the Chief of Staff of the Defence Forces, Vice Admiral Mark Mellett

(DSM) and all of the officers of the Defence Forces who assisted the Review; the Chairman of the Revenue Commissioners, Mr. Niall Cody and his team, particularly Mr. Joe Ryan; the Chairperson of the Garda Síochána Ombudsman Commission, the Honourable Ms Justice Mary Ellen Ring of the High Court, Ms Carmel Foley, Member of the Garda Síochána Ombudsman Commission and their colleagues; Mr. Pat Kenny, Member of the Competition and Consumer Protection Commission, and Mr. Sean Murphy, Legal Adviser; and the Data Protection Commissioner, Ms Helen Dixon and her colleagues.

My thanks also to the Director of Public Prosecutions, Ms. Claire Loftus and her colleagues for her assistance in understanding the use of retained communications data in criminal prosecutions.

The Irish Human Rights and Equality Commission made a considered submission to the review and I am grateful to the Chief Commissioner, Ms. Emily Logan, and her colleagues for it. Thanks are also due to the Irish Council for Civil Liberties for its submission.

The Review engaged with communications service providers in its work. I am indebted to them for their very generous assistance and would like to thank: Mr. Pat Galvin and Ms Maureen King of Eir; Ms. Edel Briody and Mr. Gary Healy of Vodafone; and Mr. Paul Durrant, Chief Executive of the Internet Service Providers Association of Ireland.

I am also grateful to the National Union of Journalists for its submissions which helpfully provided the Review with a journalist's perspective on the issues, and Newsbrands Ireland for its submissions representing the views of the newspaper industry.

I had assistance in researching the law relevant to the Review from Dr Tom Daly, Mr. Gary Fitzgerald BL and Ms. Joanne Williams BL for which I am most grateful.

Special thanks are also due to Mrs. Marjorie Johnson for her tireless and patient secretarial efforts in putting the report together while carrying the burden of being the only full-time assistant to the Review. My thanks also to Mr. Kevin McCarthy for all his support work.

John L Murray

CHAPTER ONE: OVERVIEW

INTRODUCTION

"[N]ational laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression." (Report of Special Rapporteur, Frank La Rue, United Nations, 2013, at paragraph 3).

Terms of Reference

1. The Terms of Reference of the Review are as follows:

> *"To examine the legislative framework in respect of access by statutory bodies to communications data of journalists held by communications Service Providers, taking into account the principle of protection of journalistic sources; the need for statutory bodies with investigative and/or prosecution powers to have access to data in order to prevent and detect serious crime; and current best international practice in this area."*

2. The Review was established by the Minister for Justice following a decision of the Government. This decision was made in the wake of public debate following reported access by the Garda Síochána Ombudsman Commission (hereinafter GSOC), under the aegis of the Communications (Retention of Data) Act, 2011 (hereinafter the 2011 Act), to the communications records of journalists for the purpose of identifying journalistic

sources. Media reports in January, 2016[1] indicated that GSOC investigators had accessed the telephone records of certain journalists in the context of an investigation into an alleged wrongful disclosure of information by a member of the Garda Síochána contrary to section 62 of the Garda Síochána Act, 2005. Section 62 makes it an offence for a member of the Garda Síochána (or a member of its civilian staff or someone contracted to it) to disclose information obtained in the course of carrying out his or her duties. The media reports referred to an allegation of unauthorised disclosure to journalists by a member of the Garda Síochána of information concerning an investigation into the death of a young woman in 2007. Ministerial concerns about the implications of the use of such powers for the freedom of the press led to the establishment of this Review.

Mass Surveillance

3. The importance and scope of the issues arising in this Review stem from the fact that the statutory framework referred to in the Terms of Reference – and described in detail below - establishes a form of mass surveillance of virtually the entire population of the State, involving the retention and storage of historic data, other than actual content, pertaining to every electronic communication, in any form, made by anyone and everyone at any time. Electronic communications in this context comprehend all forms of telephone (both fixed line and mobile) and internet communication, including text messages. The data retained includes location data of the caller and the person called. By virtue of the Communications (Retention of Data) Act 2011, communicationsService Providers are obliged to retain and store this corpus of private information – known as metadata in

[1] http://www.irishexaminer.com/viewpoints/columnists/michael-clifford/journalists-investigated-gsoc-powers-need-to-be-reined-in-376891.html

http://www.irishtimes.com/news/crime-and-law/gsoc-trawls-journalists-phone-records-in-inquiry-1.2495959

information technology – relating to everyone's telephone calls, text messages, e-mails and communications on the Internet. In essence, this means the retention of all communication data not going explicitly to content: in other words, data pertaining to such matters such as the date, time and location of a telephone call. In the result, a vast amount of private information pertaining to the personal communications of virtually everyone in the State is now retained without the consent of those affected in databases maintained by each private Service Provider in fulfillment of its statutory obligations, in particular those created by the 2011 Act.

4. As is explained later, the current statutory framework governing these arrangements has many of the characteristics of the kind of legislation examined by the European Court of Justice (ECJ) in the *Tele 2* case (cited later) of which the Court observed:

> *"… The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance." (Tele2 case, at paragraphs 98 and 100 of the Judgment).*

Scope and Volume of Data Retained

5. A vivid illustration of the sheer scale of the current data retention system can be gleaned from the following statistics. In 2016 over 5 billion text messages were sent in Ireland; a somewhat higher number were sent in 2015. Given that the relevant retention period is two years, this means that at any given time private companies who provide electronic communication services will have retained data pertaining to in excess of 10 billion text messages – any of which may be accessible, in defined circumstances, by State investigatory authorities, the statutory bodies referred to in the Terms of Reference. By the end of 2016 the total number of mobile telephone subscriptions had reached 5,969,928,

while the number of fixed line subscriptions stood at 1,805,923[2]. In the result, service providers are in possession of retained communications data pertaining to all of the telephone calls associated with nearly 8 million telephone subscriptions. Data is also automatically retained in respect of all internet communications, for which the retention period under the 2011 Act is one year.

6. Since this arrangement is effectively universal and indiscriminate in application and scope, it follows that it also affects the retention and storage of journalists' communications data, whether pertaining to communications between journalists or between journalists and others.

7. The private information thus retained by Service Providers is not a snapshot of information concerning a particular communication or recent communications but constitutes an historical record of all communication over a lengthy period. As already indicated, by virtue of section 3 of the Communications (Retention of Data) Act 2011, data relating to telephone communications must be kept for two years, while Internet data must be retained for one year. Although routinely referred to in anodyne terms as 'data' or 'retained data', this vast store of private information touches every aspect of an individual's private and professional communications profile over a lengthy period, including the type, source and destination of every communication made, the date, time and duration of each communication, details of the user's communication equipment, and the location of mobile communication equipment. The names and addresses of subscribers and registered users may also be identified, as well as the calling telephone number, the number called and an IP address for Internet services.[3]

---

[2]The figures are based on information from the Commission for Communications Regulation; Quarterly Key Data Report, 2/4/2016 (Reference ComReg 17/15(R) : 16/03/2017). Subscribers may have multiple subscriptions.

[3]See cases C-293/12 and C-594/12, EU:C2014:238*, Digital Rights Ireland Limited v Ireland & Others; Karntner Landesregierung v Seitlinger & Others*: Judgment of 8 April 2014, para 26.

8. Storage of the kinds of communications data mentioned in the preceding paragraph has a special importance when considering the principle of protection of journalistic sources. Data pertaining to the time, date, location, destination and frequency of a journalist's telephone calls may allow conclusions to be drawn about the recent pattern of his or her social and professional life, including his or her contacts, and thus provide a clear pathway to identifying his or her journalistic sources.[4] For example, location data linking a journalist's telephone calls with those of another caller in the vicinity of, say, Leinster House before or after a sensitive meeting in which that person was known to have been involved, might well be thought crucial in this regard.

Digital Rights Ireland

9. It should be noted at the outset that the 2011 Act was enacted to give effect to EU Directive 2006/24 on the retention of data generated by public electronic communications.[5] The Directive obliged Member States to adopt measures to ensure that communications data, including location data, are retained in accordance with its provisions. In 2014 the European Court of Justice (ECJ) declared Directive 2006/24 to be invalid, broadly speaking because the Directive, as an EU legislative measure, failed to make express provision for sufficient safeguards for the protection of the fundamental rights of citizens as guaranteed by the European Charter of Fundamental Rights. The decision of the Court declaring the Directive invalid was made in the case of *Digital Rights Ireland.*[6] This case, which is reviewed in Chapter 2, arose from a reference to the ECJ by the High Court of Ireland, pursuant to Article 264 of the Treaty on the Functions of the European Union. The ECJ found that the system of data retention envisaged by the

[4] See note 3 at para 99 of the Judgment.

[5] Directive 2006/24/EC, 15 March, 2006 "On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks …"

[6] *Digital Rights Ireland v Minister for Communications and Others:* Joined cases C-293/12 and C-514/2. The other of the joined cases was a reference from an Austrian court.

Directive constituted a disproportionate interference with the fundamental rights guaranteed by the Charter because it lacked sufficient safeguards protecting fundamental rights. Crucially, the Court did not find that the *scope* of the system as such was incompatible with EU law.

10. Having declared that Directive 2006/24EU on the retention of communications data was invalid, the decision of the ECJ in *Digital Rights Ireland* nonetheless left open, or undecided, several issues fundamental to the operation of a compulsory communications data retention regime under the national laws of member states (even where the latter were intended to implement the Directive). These unresolved issues included whether EU law generally, and in particular Directive 2002/58 on the protection of privacy in electronic communications, applied to implementing national legislation. Moreover, even in the event that it did, a significant number of Member States took the view (as they were later to argue in *Tele2*) that EU law did not apply to the conditions under which state bodies, such as police forces, were entitled to access retained communications data.

11. As the judgment of the ECJ in *Digital Rights Ireland* left open a significant range of arguable implications for national legislative measures, it followed that there was no determining judicial decision on these issues under EU law; and this in turn meant that the initial focus of the Review was necessarily expansive both in regard to the standards and safeguards which a state might be obliged to observe when operating a regime of indiscriminate communications data retention, and in respect of the international reference points for determining such standards.

Impact of *Tele2*

12. In its seminal judgment of 21 December 2016 the Court of Justice of the European Union in *Tele2* examined the compatibility with EU law of certain national enactments establishing a system of indiscriminate communications data retention, with particular regard to certain

fundamental rights guaranteed by the EU Charter of Fundamental Rights.[7] The judgment, which is discussed in detail in Chapter 2, turns on two fundamental conclusions. First, it significantly reduced the permissible scope of the statutory obligations that can be imposed on Service Providers to retain the communications data of subscribers without their consent. The Court held that the existing forms of automatic and wholly indiscriminate retention of private communications data cannot be reconciled with European law. It concluded that retention can only occur, exceptionally, in pursuit of the objectives which are exhaustively listed in Article 15(1) of Directive 2002/58[8], and cannot be wholly indiscriminate without exception, in scope and application. Second, the Court decided that access to retained private data by state bodies is only permissible where strictly necessary for one of the objectives set out in of Article 15 (1), and then only when accompanied by robust safeguards protecting the fundamental rights affected by it.[9] As will be seen later, the first of these conclusions effectively sweeps the ground from under wholly indiscriminate mass surveillance schemes of the kind established by the Communications (Retention of Data) Act 2011. In light of *Tele2*it may no longer be lawful to compel Service Providers to retain all private data as part of a general, wholly indiscriminate surveillance scheme applying to everyone who communicates by telephone or via the internet.

---

[7]See cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-Och Telestyrelsen; and Secretary of State for the Home Department v Watson & Others:* Judgment of 21 December, 2016.

[8]Article 15 (1) provides "1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to **safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system,** as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

[9]At para 134 of the Judgment.

13. The second seminal conclusion- that EU law is applicable to the circumstances and conditions under which state bodies may *access* retained communications data - has far-reaching implications for the rules currently governing such access, and, indeed, for any future scheme that may be fashioned in this area in light of the conclusions and recommendations set out in this Review.

14. It should however be stressed that the decision in *Tele2* does not appear to preclude Member States from taking proportionate action in the use of communications data in the fight against serious crime and terrorism, or in respect of the other objectives identified in Article 15 (1) of Directive 2002/58.

15. Moreover, the decision in *Tele2* also appears to accept that a data retention scheme that is not wholly indiscriminate – without any exception - would be compatible with European law provided certain objectively verifiable conditions were clearly satisfied and necessary safeguards provided. In this regard, the ECJ specifically referenced a scheme limited by geographic region in respect of which it was possible, ''based on objective evidence…to identify a public whose data is likely to reveal a link…with serious criminal offences…or to preventing a serious risk to public security.''[10]It goes without saying that is for the Oireachtas to decide, as a matter of policy, what this rubric might mean in the context of domestic law, although it will be suggested that a statutory scheme providing for data retention orders limited by topography or even by locality in the wake of a terrorist attack or on foot of credible evidence of an imminent attack would fall within its ambit.

Inherent Risks

16. Although the communications data retained under the Act of 2011, often referred to as metadata, never includes the content of communications, collectively the retained data

[10]At para 111 of the Judgment.

constitutes vital and comprehensive information concerning the private lives and professional activities of everybody, without exception. Section 2 of the 2011 Act expressly excludes the contents of communications from its application. Other legislation that permits a form of "targeted surveillance" against individuals, including access to the contents of their communications, falls outside the scope of this Review. (See paragraphs 25-27 below.)

17. In giving effect to Directive 2006/24/EC, the 2011 Act obliges the providers of communications services (the Service Providers) indiscriminately to collect and retain electronic communications data which, as the ECJ pointed out in *Tele2*, "*provides the means … <u>of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications</u>* (emphasis added). Accordingly, the fact that the regime of communications data retention established by the 2011 Act does not apply to the content of communications does not mean that the Act's interference with a person's right to privacy and other affected fundamental rights is any less serious on that account.

18. In this regard, the Court of Justice in *Tele2*expressly endorsed (at paragraph 99 of the Judgment) statements made by the Advocate General in the same case: viz, "I would emphasise that the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications …In particular, as the examples I have given demonstrate, 'metadata' facilitate the almost instantaneous cataloguing of entire populations something which the [storage of the] content of communications does not". The Court also made reference to a similar assessment made in a recent report by the United Nations High Commissioner for Human Rights.

19. In similar vein, a United Nations Special Rapporteur in a Report on the implications on compulsory retention of communications data observed[11]:

> *"The communications data collected by third-party Service Providers, including large Internet companies, can be used by the State to compose an extensive profile of concerned individuals. When accessed and analysed, even seemingly innocuous* transactional records *about communications can collectively create a profile of an individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as or even greater detail than would be discernible from the content of communications alone. By combining information about relationships, location, identity and activity, states are able to track the movement of individual and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with."*

20. By way of illustrating the political risks associated the mass retention of so-called metadata, the Advocate General in the *Tele2* case stated:

> *"257. Let us suppose, first of all, that a person who has access to retained data wishes to identify all the individuals in the Member State who have a psychological disorder. Analysing the content of all communications effected within the national territory for that purpose would require considerable resources. On the other hand, by using databases of communications data, it would be possible instantly to identify all the individuals who have contacted a psychologist during the data retention*

[11]Report of the Special Rapporteur on the Promotion and Protection of the Right to freedom of Opinion and Expression, Frank La Rue, 17 April 2013; United Nations General Assembly A/HRC/23/40, para 42.

period. I might add that that technique could be extended to any of the fields of specialist medicine registered in a Member State.

258. Now let us suppose that that same person wished to identify individuals opposed to the policies of the incumbent government. Again, analysing the content of communications for that purpose would require considerable resources, whereas, by communications data it would be possible to identify all individuals on the distribution list of emails criticising government policy. Furthermore, such data would make it possible to identify individuals taking part in any public demonstration against the government."

21. Accordingly, even though the content of private communications is not affected by its provisions, the mandatory data retention scheme established by the 2011 Act means that an important historical record of personal information about every communications user in the State must be stored by and under the exclusive control of private communications Service Providers. It is then subject to access by statutory bodies in accordance with the provisions of the Act. Both in scope and timescale, the information stored goes well beyond what might normally be done by commercial or State entities for billing or administrative purposes. Moreover, data retained for billing or administrative purposes would normally be confined to personal information – such as name and contact details – relevant to those purposes, and must be destroyed when no longer required. Thus the Data Protection Acts set strict limits on the length of time such personal data may be kept for purely administrative purposes.

22. As already indicated, the 2011 Act is universal and indiscriminate in reach and application. It applies to all telephone and Internet communications made by every person within the State. Accordingly, data files are retained on all communications users without their consent; and although this Review is directly concerned with its impact on journalists, the Act makes no distinction between journalists and other communications users - or, for that matter, between communications users generally and other groupings, such as members

of the Oireachtas, the Judiciary, Government ministers, trade unionists, medical doctors, teachers, sports club members etc. All are subject to the regime of compulsory communications data retention established under the Act.

23. Insofar as communications data may legitimately be retained for such purposes as the investigation or prosecution of serious crime, it follows that the provisions of the 2011 Act apply to everyone and anyone - including journalists - reasonably suspected of being involved in the commission of crime. By the same token, the fundamental rights enjoyed by journalists in respect of the retention and disclosure of their communications data, both personal and professional, are the same as those enjoyed by citizens generally. Journalists enjoy those rights as citizens, not by virtue of their occupation or professional activities as journalists. Accordingly, journalists are entitled to the same legal protections and safeguards as everyone else in the matter of their private or professional communications, whether these arise under Irish law, E.U. law or the European Convention on Human Rights.

24. Thus it what follows the data retention and disclosure system established by the 2011 Act is examined in terms of its impact on citizens generally, with a view to identifying, for the benefit of citizens and journalists alike, the fundamental rights threatened by its operation as well as the reforms and safeguards needed to protect those rights in the future. Special considerations for journalists do however arise in connection with the principle of protection of journalistic sources as referred to in the Terms of Reference. Not least of these is a concern that the 2011 Act appears to permit access to a journalist's retained data for the purpose of uncovering his or her sources even in the context of investigating a suspect other than the journalist. Accordingly, the issue of the confidentiality of journalistic sources is treated separately, and is the subject of a number of specific recommendations.

Targeted Surveillance

25. It is important to distinguish the data retention scheme set out in the 2011 Act from the various forms of targeted electronic surveillance countenanced in other enactments – such as the Criminal Justice (Surveillance) Act 2009 or the Interception of Postal Packets and Communications Messages (Regulation) Act 1993– which do not come within the scope of this Review. As already indicated, the latter, unlike the former, are neither universal nor indiscriminate, but involve the surveillance of a particular suspected person for the purpose of investigating or preventing serious crime or maintaining the security of the State. Thus, targeted surveillance can arise where the Garda Síochána have reasonable grounds for suspecting a particular person has been involved in the commission of criminal offences and wish to carry out current and ongoing surveillance of the suspected person's communications, including the contents thereof. This may take the form of what is sometimes popularly referred to as "telephone tapping".[12]

26. In contrast, mass surveillance involving the indiscriminate retention and storage of communications data affects every communication of every person, even of those that are neither suspected nor ever likely to be suspected of any wrongdoing. Access by statutory bodies, such as the Garda Síochána, to historical private data already retained and stored by private communications companies arises when such a body itself decides that there are grounds for suspecting a particular person of being involved in unlawful activity relating to the commission of serious crime or the security of the State. Moreover, under current legislation it is considered permissible to access a person's communications data for the purpose of investigating an offence suspected of having been committed by another person.

---

[12] Somewhat confusingly, one finds that the ECJ in its judgment in the *Tele2* case uses at one point a reference to "targeted" retention of data. As is explained later in the Review, the use of "targeted" in this context has quite different connotations from the general concept of "targeted surveillance" referred to above.

27. Finally, targeted surveillance can only be authorised by an independent authority, and the grounds of suspicion on which it is sought must be shown to be reasonable. No such limitations govern the system of automatic and indiscriminate surveillance established under the 2011 Act. On the contrary, under that system communications data is routinely stored irrespective of the activities, even if lawful and innocent, of the persons to whom it relates; and neither the retention of, nor subsequent access to, such data by statutory bodies is subject to prior authorisation by a judge or independent body.

International Practice

28. The risks inherent in systems of automatic and mass retention of electronic communications data have been canvassed by constitutional courts in many countries including Ireland, and by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (ECJ). The case law of the ECJ is of particular and obvious importance as it is specifically concerned with the kind of data regime established by the 2011 Act and, as explained later, because of its conclusions, both with regard to the compatibility of such a regime with fundamental rights and the necessity for safeguards to protect such rights, are binding on the State. Of the two judgments of the ECJ which directly addressed the kind of data retention regime established by the Act of 2011, the first was the *Digital Rights Ireland* case which arose from a reference to the ECJ from the High Court of Ireland which was concerned with the validity of E.U. legislation, namely, the 2006/24 Directive on Data Retention. The second and more important judgment of the ECJ is that given in the *Tele2*case which, unlike *Digital Rights Ireland* (which was concerned with the compatibility of an EU Directive with the higher norms of EU law), directly addressed the compatibility with EU law of national legislation establishing a wholly indiscriminate system of communications data retention.

29. The Terms of Reference refer to “current best international practice” in the area of obligatory retention of communications data, and it is convenient to point out at this stage that the case law of the ECJ will be treated as the primary source of what may be considered as the best international practice in this regard. In the first instance this is on

account of the primacy of EU law over national law and the fact that the ECJ has now held that EU law, including the European Charter of Fundamental Rights, applies both to the nature and scope of any general form of communications data retention and to the conditions under which such retained data may be accessed by State authorities at national level. A secondary reason is the fact that the ECJ in its judgments, and particularly in its recent judgment in the *Tele2* case, took account of international practices and standards, including those set by the ECHR, in this area, when setting the criteria, safeguards and practices which should be observed by a Member State. Furthermore, the primacy of EU law means that the decisions of national courts, including the Irish courts, (although they have made important pronouncements touching issues in this area) are not strictly pertinent given the all-embracing and defining principles of applicable EU law as set out in the *Tele2* case. That said, regard should be had, in parallel, to the principles and standards derived from the case law of the ECtHR, given that the State has concurrent obligations to protect fundamental rights under the European Convention on Human Rights.

30. What emerges from consideration of the relevant international sources (viz., judicial decisions and dicta, and the opinions and conclusions expressed by international bodies) is that the very existence of indiscriminately assembled historical databases gives rise to a real risk of abuse of access to them, as well as misuse of information contained in them, both by individuals and/or State authorities. The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has also pointed out that, by compelling communications Service Providers to create large bodies of retained data, *governments have not only broadened the scope of state surveillance and the possibility of human rights infringements, they have also created a significant risk of "theft, fraud and accidental disclosure" of their contents*.[13] There is also a risk that, without

[13] See note 4 above at para 67.

adequate safeguards, personal data bases are vulnerable to arbitrary or even unregulated access. (Emphasis added)

31. The potential threat to fundamental rights and freedoms arising from the statutory rights of access to retained data by state investigatory authorities is especially concerning and full consideration is given to these arrangements when dealing with the detailed provisions of the 2011 Act.

32. It is not a matter of controversy to observe that any statutory system of access to retained communications data must be accompanied by effective safeguards against abuse. Indeed, the 2011 Act recognises this to some extent by limiting and regulating the circumstances in which retained data may be accessed by statutory bodies; although it is clear, particularly in light of the decision in *Tele2*, that many of these safeguards do not meet EU or international norms and standards. It should be added at this point that the statutory bodies (referred to in more detail below) which have been given powers of access under the 2011 Act are themselves conscious of the need to avoid abusing or misusing their powers, and that each has put in place administrative procedures designed to ensure that existing safeguards, so far as they go, are properly observed.

33. Nonetheless, the effectiveness of safeguards, in particular those of a purely administrative nature, may be undermined by the myopic views of an investigatory agency on the nature and implications of surveillance by means of the mass retention of historical communications data. There is an inherent risk that investigatory bodies would regard access to a person's private communications data as something to which they are entitled as of right any time that it may appear, in their light, useful for their purposes. Access to a person's private historical communications data is an intrusion on their rights and on data which is personal to them. In accordance with national, EU and international laws, access to such private data must be governed, *inter alia*, by the principle of proportionality, that is to say, it should be permissible only when it is strictly justified or necessary for legitimate public interest purposes and when no other less intrusive means of achieving such purposes is reasonably available. Mere utility or potential utility is not the test.

34. Morever, it will be seen in Chapter 3 that administrative safeguards are not enough in this context as there is an ever-present risk that they will be undercut by the demands and exigencies of investigatory agencies for access to retained communications data in pursuit of their own objectives.

35. The impact of data retention regimes on human rights has also been the subject of discussion and debate throughout the democratic world. On this issue the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has noted that:[14]

> *"L. Innovations in technology have facilitated increased possibilities for communication and freedom of expression, enabling anonymity, rapid information sharing, and cross-cultural dialogue. At the same time, changes in technologies have provided new opportunities for State surveillance and intervention into individuals' private lives.*
>
> *…*
>
> *Innovations in technology throughout the twentieth century changed the nature and implications of communications surveillance.*
>
> *15. The dynamic nature of technology has not only changed how surveillance can be carried out, but also 'what' can be monitored. In enabling the creation of various opportunities for communication and information-sharing the Internet has also facilitated [in addition to the transition from fixed-line telephone systems to mobile communications] the development of large amounts of transactional data about individuals*. This information, known as communications data or metadata, *includes*

[14]See note 4 above.

personal information on individuals, their location and online activities, and logs and related information about emails and messages they send or receive. Communications data are storable, accessible and searchable, and their disclosure to and use by state authorities are largely unregulated. Analysis of this data can be both high revelatory and invasive, particularly when data is combined and aggregated. *As such, states are increasingly drawing on communications data to support law enforcement or national security investigations.* States are also compelling the preservation and retention of communications data to enable them to conduct historical surveillance.

…

Over time, however, States have expanded their powers to conduct surveillance, lowering the threshold and increasing the justification for such surveillance.

17. In many countries, existing legislation and practices have not been reviewed and updated to address the threats and challenges of communications surveillance in the digital age. *… Today, in many States, access to communications data can be conducted by a wide range of public bodies for a wide range of purposes, often without judicial authorisation and independent oversight. …*

18. Human rights mechanisms have been equally slow to assess the human rights implications of the Internet and new technologies on communications surveillance and access to communications data. The consequences of expanding States' surveillance powers and practices for the rights to privacy and freedom of opinion and expression, and the independence of those two rights, have yet to be comprehensively considered by the Human Rights Council. … This Report seeks to rectify this." (emphasis added)

36. The Rapporteur went on to reflect on the need for a robust assessment of the human rights implications of the new technologies on communications surveillance and access to communications data.[15] This concern is also a focal point of this Review, with special emphasis being given to the impact of mass surveillance technologies on the rights of journalists – including the principle of protection of journalistic sources and the wider issues of freedom of expression and freedom of the press.

Role of Fundamental Rights

37. It has already been pointed out that the statutory framework mandating communications retention constitutes a serious threat to fundamental rights as recognised in the Irish Constitution, the European Union Charter on Fundamental Rights and the European Convention on Human Rights and Fundamental Freedoms. The statutory regime governing the retention and disclosure of private communications data accordingly falls to be evaluated in light of the fundamental rights affected by its operation. This approach will enable the Review to identify the degree to which, if at all, large-scale data retention is possible, particularly following the decision of the ECJ in *Tele2*; while at the same time focusing on the safeguards necessary to protect against the undue infringement of personal rights necessarily involved in the storage and disclosure of personal data. Accordingly, the human rights dimension of data retention regimes is a constant theme in the substantive parts of the Review.

Public Interest, Crime and State Security

38. Fundamental rights are not, generally, absolute. The State has a legitimate interest in using reasonable means to combat crime in all its forms, including organised crime, terrorism and other activity that may pose a specific threat to the security of the citizen

[15] At para 18.

and the State. The more serious the crime the more important it is that the State has such means available to its law enforcement agencies. Moreover, it goes without saying that society has a legitimate expectation that the State will act effectively and proportionately in protecting it against the threat of criminality and terrorism.

39. In pursuing the foregoing objectives all democratic countries founded on the rule of law recognise that the state may interfere with fundamental rights in the pursuit of such legitimate public interest objectives. Generally speaking, the State may only limit or restrict the protection or exercise of fundamental freedoms for legitimate public interest purposes provided the measures are proportionate so as not to affect the essence of such rights and are limited to what is necessary in a democratic society. Again, there can be no issue that the protection, investigation and prosecution of serious crime, including unlawful activity posing a real and serious threat to the security of the state, constitute purposes for which proportionate and necessary interference with fundamental rights may be considered permissible.

Balancing Security and Personal Rights

40. It follows that a balance has to be struck between ensuring that the state and its authorities have effective and legitimate tools at their disposal in the fight against serious crime and threats to the security of the state, on the one hand, and the protection of fundamental rights and freedoms, on the other. Although the broad parameters of this balance are often self-evident, difficult issues arise when attempting to draw precise borders between them. These difficulties arise in the first instance for legislators seeking to enact public interest measures that have an impact on personal freedoms, and ultimately for the courts should such measures be the subject of constitutional or judicial review.

41. By the same token, it follows that statutory powers trenching on individual rights must be accompanied by appropriate measures safeguarding the affected rights to the fullest extent possible consistent with the legitimate public interest objectives being pursued.

Safeguarding rights in such circumstances is necessary to protect against disproportionate interference as well as the arbitrary exercise, misuse or abuse of the statutory powers by State bodies.

42. It is a matter for the Oireachtas in the first instance to determine whether and to what extent legislation may interfere with the exercise of fundamental freedoms subject to what is permissible under the Constitution, under the law and treaties of the European Union where applicable, and with due regard to the state's obligations under the European Convention on Human Rights and Fundamental Freedoms.

43. In short, this is essentially a policy consideration falling within the domain of the legislature, albeit that legislation in most democracies founded on the rule of law may be subject to judicial review as regards its compatibility with higher norms such as a constitution or EU law or international treaties having direct force in domestic law.

44. This Review of the statutory framework governing access to private communications is not in any sense akin to judicial review of existing legislation. Nor is it concerned with the drafting of future legislation, even if some of the analysis contained in it may have implications for new or amending legislation in the event that either of the latter is considered necessary. Similarly, as has already been pointed out, the Review does not deal with any of the other statutory surveillance powers giving the Garda Síochána or the Defence Force access to the contents of communications for the purposes of investigating crime, or to information gleaned as a result of the lawful seizure of communications equipment.

45. Rather the Review proceeds on the policy assumption, reflected in existing legislation (and expressly stated in the Terms of Reference) that there is a need that certain statutory bodies, essentially law enforcement agencies, be given some access to the retained communications data of private persons including journalists but only for legitimate public interest purposes which include the detection, investigation and prosecution of serious criminal offences and criminal activity relating to the security of the State.

46. Thus the aim of the Review is to examine the legislative framework in this domain; to identify the fundamental rights and freedoms of journalists affected by it; and to outline the safeguards which ought to be built into legislation affecting those rights and freedoms; while at the same time permitting the pursuit of the legitimate objectives of combating serious crime and unlawful threats to the security of the State.

47. Accordingly, the principal focus in what follows is the regime established under the Communications (Retention of Data) Act 2011 enjoining the automatic collection and storage of communications data originating or terminating within the state. In the nature of things, consideration will also be given to the impact of the recent decision of the European Court of Justice in *Tele2* on the regime of automatic information storage underpinning the 2011 Act. As already indicated, in that case the ECJ decided that communications data may only be retained and accessed when strictly necessary for the prevention of serious crime and terrorism, and for other prescribed purposes; and, consequently, that the universal and indiscriminate storage of communications data is unlawful. On this reasoning, the current system of indiscriminate data retention underpinning the 2011 Act does not appear to be sustainable. The decision in *Tele2*is discussed in detail in Chapter 2.

48. It should however be noted that the provisions of the Communications (Retention of Data) Act 2011 are for the time being unaffected by the decision in *Tele2*. As matters stand, although the decision in the case of *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources & Others*[16] invalidates the EU Directive which the 2011 Act purports to implement, the 2011 Act remains part of the law of the State. It constitutes the core of existing statutory framework governing retention and disclosure of communications data. Moreover, given the Review's Terms of Reference, it

[16]Joined cases C-293/12 and C-594/12

provides a necessary starting-point for any future statutory scheme that might be contemplated in light of the criticisms, conclusions and recommendations set out in respect of it in this Review.

KEY CONCEPTS AND CONCERNS

Legislative Framework

49. The Terms of Reference specifically refer to the ''legislative framework'' governing the retention of ''communications data''; to ''Service Providers'' charged with the storage of such data; to ''statutory bodies'' with a right of access to it; and to the ''principle of protection of journalistic sources'' in the context of data retention. The meaning and scope of these concepts are considered briefly here, pending closer scrutiny when the provisions of the 2011 Act are examined in detail later in the Review.

50. By and large, the term legislative framework refers to the scheme established by the Communications (Retention of Data) Act 2011 (as amended), which imposes an obligation on communications Service Providers to collate and store metadata pertaining to all telephony and internet communications occurring within the state. The relevant data is thus generated by the simple fact of making or receiving a communication by telephone or on the internet. The resultant data is then stored, without the consent of those affected, in a manner, and for periods, that would be unlawful but for the provisions of the 2011 Act.

51. While the 2011 Act of constitutes the bulk of the applicable law governing the retention of electronic data, the following statutory provisions are also relevant: section 98 of the Garda Síochána Act 2005, invoked by the Garda Síochána Ombudsman Commission for the purpose of accessing retained data under the 2011 Act; sections 1-8 of the Data Protection Acts 1988, 2003, as amended; section 75 of the Criminal Justice (Mutual Assistance) Act 2008; and section 98 of the Postal and Telecommunication Services Act 1983, as amended. It is important to note that the 2011 Act has been significantly amended by section 89 of the Competition and Consumer Protection Act 2014 to provide the Competition and

Consumer Protection Commission with the power to make disclosure requests under section 6 of the 2011 Act in relation to certain competition law offences, and to provide for related matters. The 2011 Act has also been amended by Regulation 52 of S.I. No. 349/2016 - European Union (Market Abuse) Regulations 2016. This has added certain insider trading offences under Regulation 5 and 7 of the European Union (Market Abuse) Regulations 2016 to Schedule 1of the 2011 which deems offences to be "serious offences".

52. The term ''statutory bodies'' refers to those entities enjoying access to retained data under section 6 of the 2011 Act., viz:

- The Garda Síochána (also by virtue of section 8(b) of the Data Protection Acts 1988 and 2003, as amended);
- The Defence Force;
- The Revenue Commissioners;
- The Data Protection Commissioner (by virtue of section 5(d) of the 2011 Act);
- The Competition and Consumer Protection Commission (by virtue of section 6(3A) of the 2011 Act as inserted by section 89 of the Competition and Consumer Protection Act 2014);
- The Garda Síochána Ombudsman Commission – GSOC (by virtue of section 98 of the Garda Síochána Act 2005);

The terms of access given to the aforementioned bodies by the 2011 Act, together with the separate terms relied on by GSOC in this connection, are examined in detail later in the Review.

53. As used in the Terms of Reference, the phrase ''communications data'' refers to information on the identity and location of a person making or receiving a telephone or Internet communication. In other words, it refers to the traffic and location information which Service Providers are obliged to store – for periods of two years in respect of telephone communications, and one year in respect of Internet communications. As already indicated, the provisions of the 2011 Act in this regard are examined in detail below. Suffice it to say for present purposes that the term communications data refers to the total mass of communications data retained under the 2011 Act; and that the collection and retention of such data by Service Providers is made mandatory and indiscriminate by the Act, and thus is not limited to data tainted by suspicion of criminal activity or by any other consideration.

54. The term ''Service Provider'' references the definition in section 1 of the 2011 Act: viz., ''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.''

Journalists and the Protection of Sources

55. The Terms of Reference refer specifically to access by statutory or investigatory bodies to the communications data of journalists, and to the need to take account 'the principle of protection of journalistic sources' in this context. The issue of protecting journalistic sources is important, and will be discussed separately, albeit in the wider context of the retention and storage of the communication data of all users of telephony and data transmission systems.

56. How is the term "journalist" to be defined? In light of the diversification of modern media and communications, this has become a difficult question to answer with precision. As the Parliamentary Assembly of the Council of Europe has observed, just as "… the media landscape has changed through technological convergence, the professional profile of journalists has changed over the last decade. Modern media rely increasingly on mobile

and Internet-based communications services." [17] Accordingly, the modern notion of journalism must extend beyond traditional perceptions of work in the domain of print news publications or mainstream broadcasting. An obvious example of the newer form of journalism is to be found among those who write and maintain blogs on the internet and, indeed, other forms of professional publishing on the internet.

57. It should first of all be noted that all journalists, however one defines the term, enjoy, as citizens or persons within the State, the full panoply of protections and guarantees afforded by the law, including the Constitution, EU law, and the ECHR, to fundamental freedoms such as the right to privacy, the right to freedom of expression and the right to communicate. These rights and freedoms are enjoyed by journalists not because they are journalists, but as citizens or persons conducting lawful activity within the State.

58. Accordingly, a definition of the term journalist is relevant for present purposes only where, and to the extent that, it is envisaged that some special statutory protection should be afforded to journalists due to their status or activities as journalists, over and above the rights and protections they are entitled to as citizens. As reflected in the Terms of Reference, the possible need for special protection for journalists arises in connection with their role as tribunes of the public interest as facilitated by "the principle of protection of journalistic sources.''

59. For the purposes of this Review it is proposed to adopt the definition contained in the Council of Europe Recommendation No. R(2000)7 of the Committee of Ministers on the Rights of Journalists Not to Disclose their Sources of Information:

[17] Recommendation 1950 (2011) of the Parliamentary Assembly on "The Protection of Journalists' Sources".

> *"The term 'journalist' means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication;"*[18]

60. Similarly, the Review proceeds in accordance with the principle:

> *"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."*[19]

61. This principle is reflected in the laws and judicial dicta of many democratic states and several international instruments on journalistic freedoms including Article 10 of the European Convention on Human Rights and Fundamental Freedoms. In line with the Terms of Reference, the principle will be taken into account when reviewing the legislative framework providing access by statutory bodies to journalists' communications data and when assessing the need for additional statutory protections for journalists in this context.

62. By the same token, it will be seen that the Terms of Reference acknowledge that access to journalists' telecommunication data may also impact on their rights as citizens; hence the subsidiary role they assign to consideration of the protection of sources issue. As matters stand, journalists are vulnerable to the disclosure of information that, while it may have no bearing on their professional activities, and/or does not in any way compromise their sources, nevertheless significantly affects their rights as private citizens – as would be the case, for example, where disclosure constituted an unwarranted breach of the right to privacy. For this reason, in addition to its focus on the special position of journalists, the overarching concern of the Review is with those features of the data retention scheme

---

[18]Adopted by the Committee of Ministers of the Council of Europe on 8th March, 2000, Appendix.

[19]*Goodwin v United Kingdom* 1996 EHRR 123.

established by the 2011 Act which trench upon the wide array of rights and freedoms shared by journalists and their fellow citizens alike, as well as with the safeguards necessary to protect these rights and freedoms from undue infringement.

63. Accordingly, it is proposed to begin with a review of the relevant legislative framework from the perspective of its impact, actual or potential, on the fundamental rights of citizens generally and other persons lawfully within the state. As the 2011 Act makes no distinction between journalists and others in the matter of data retention, this approach has the advantage of readily identifying the plenitude of rights to which journalists are entitled as citizens, thus clearing a path for the further identification of any special additional safeguards which ought to be accorded to journalists for the purpose of protecting their sources.

Status of the Communications (Retention of Data) Act, 2011

64. As its long title makes clear, the Communications (Retention of Data) Act, 2011 was in part enacted to give effect to Directive 2006/24/EC on the Retention of Data Generated in Electronic Communications Services or Public Communications Networks. Since that Directive has since been declared invalid by the European Court of Justice in its ruling in *Digital Rights Ireland*, brief reference to what might be called the status of the 2011 Act seems appropriate in advance of outlining its provisions. As already indicated, the ECJ's subsequent ruling in *Tele2*means that a system of automatic and indiscriminate data retention of the kind established by the 2011 Act appears to be precluded by EU law. Whether the 2011 Act, in its capacity as a national legislative measure, should also be declared incompatible with EU law in light of *Tele2* is ultimately a matter for the Irish courts to decide. At the time of writing, there are proceedings still pending before the High Court – arising from a reference made to the European Court of Justice in *Digital Rights*

Ireland v. The Minister for Communications, *Marine and Natural Resources& Others*[20] – which raise fundamental issues concerning the legal effect and status of the 2011 Act. These developments notwithstanding, the 2011 Act for the time being remains in force and continues to be part of the applicable law of the state. In addition, irrespective of the ultimate fate of the Act, the analysis and recommendations pertaining to its provisions set out in this Review may well have implications for any future policy decision concerning a legislative framework fashioned by way of replacement or amendment to the existing scheme. As will be recalled, the Terms of Reference appear to contemplate the continuance of a statutory system of retained communications data in one form or another; at all events, this was the policy basis upon which the Review was established: viz., '' the need for statutory bodies…to have access to data in order to prevent and detect serious crime…''

65. It should be noted in this connection that the recent decision in *Tele2* limits the scope of any general communications data retention regime by finding that a wholly indiscriminate retention of the communications of every user, without exception, is incompatible with EU law. The direct implications of the *Tele2* case both as to the permissible scope of a data retention regime and the safeguards which must accompany even a limited form of communications data retention are examined more fully in Chapters 2 and 3, respectively.

66. Finally, it should also be noted that, notwithstanding the invalidity of the Directive underpinning it, the 2011 Act remains relevant to the central concerns of this Review as the core element of the statutory framework referred to in the Terms of Reference. Since the Act was intended to give effect to this Directive, it follows that the Act must be interpreted with due regard to its terms and intent.

[20]Joined cases C-293/12 and C-594/12

Specific Focus of Review

67. Broadly speaking, the aim of this Review is to examine the legislative framework governing the mass retention and disclosure of private communications data in light of established domestic and international legal norms, with regard to the impact of these measures on journalists generally and the protection of journalistic sources. Thus the Review is not intended to be investigatory in nature; it does not probe the manner and extent to which the current statutory system has been operated by the Service Providers mandated to retain communications data. Nor does it examine the activities of the statutory bodies that have power to access such data. Accordingly, there was no investigation of the utility and effectiveness of the current data retention system or of the extent to which it might have been used or even misused.

68. Naturally the relevant Service Providers and statutory bodies were consulted and asked to furnish information concerning the detailed operation and functioning of the system for retention of communications data and access to it. All co-operated fully with this request. In general terms, the purpose of this consultation was to gain an understanding of how the system functioned, the modus operandi of the various agencies that have a role within it, and, in particular, to get an overview of the structures and procedures which the various agencies had in place to ensure, from their perspective, that the systems of retention and disclosure functioned effectively and securely.

69. Accordingly, selected Service Providers explained how communications data was generated and stored, and securely protected from wrongful access. Similarly, the statutory bodies explained the procedures and structures they had in place with a view to ensuring as far as possible that the powers of access to such data were exercised only in accordance with law and for appropriate statutory purposes, as well as providing information on the security of data thereby obtained from Service Providers. All of the statutory bodies acknowledged, to one degree or another, the principle that powers of access to retained data should be exercised proportionately having regard, in particular, to personal rights such as the right to privacy. Nonetheless, the Review must make

recommendations concerning the safeguards, particularly those having the force of law, which should be put in place in order to ensure that the principle of proportionality is observed in practice.

70. Neither is it part of the remit of this Review to pass judgment on the compatibility of existing legislation with the Constitution, EU law or the European Convention on Human Rights and Fundamental Freedoms. It goes without saying that these are ultimately matters for the courts, albeit that the ensuing analysis of the statutory regime governing data retention has perforce been conducted with due regard to established norms and principles, and is thus in varying degrees critical of the provisions of the 2011 Act to the extent that they have been found wanting in this respect. By parity of reasoning, nor does the Review aim to provide a template for future legislative action; any conclusions drawn in this regard are intended to be purely advisory in nature.

71. Finally, it should also be borne in mind that the Review is not concerned with the powers enjoyed by the Garda Síochána or the Defence Force to intercept and monitor private communications, a practice often popularly referred to as "telephone tapping". These powers are conferred by enactments which do not form part of the statutory framework referred to in the Terms of Reference. Broadly speaking, this is because they establish a form of surveillance targeting specific individuals suspected of involvement in criminal activity, unlike the scheme created by the 2011 Act which effectively comprehends the entire population without reference to the behaviour of any individual criminal or otherwise.

COMMUNICATIONS (RETENTION OF DATA) ACT, 2011

Introductory Matters

72. As already indicated, the 2011 Act constitutes the principal component of the statutory framework governing the retention, storage and disclosure of all personal communications

data, that is to say, all traffic data or location data generated by any communication by any person, including journalists, within the State.

73. The long title to the Act describes it as:

> *"An Act to give effect to Directive No. 2006/24/EC... on the retention of data `generated or processed in connection with […] electronic communications services or of public communications networks"*

74. The long title goes on to state that one of the objects of the Act is:

> *"To provide for the retention of and access to certain data for the purposes of the prevention of serious offences, the safeguarding of the security of the State and the saving of human life"*

75. And, in this connection, that a concomitant purpose is:

> *"to repeal Part 7 of the Criminal Justice (Terrorist Offences) Act, 2005, to amend the Interception of Postal Packets and Communications Messages (Regulations) Act, 1993 and to provide for related matters."*

76. Section 1 sets out a number of definitions, the relevant ones being:

- "data" means traffic data or location data and the related data necessary to identify the subscriber or user;

- "Referee" means the holder of the office of Complaints Referee under the Interception of Postal Packets and Communications Messages (Regulation)Act 1993;

- "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. In short it means all

companies who provide a telephone service in any form or an Internet service used within the State;

- ''serious offence'' means an offence punishable by imprisonment for a term of 5 years or more, and an offence listed in Schedule 1 is deemed to be a serious offence;

- "telephone service" means calls (including voice, voicemail, conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multimedia services (including short message services, enhanced media services and multi-media services).

77. Section 2 provides that the Act does not apply to the content of communications made by telephone, fixed or mobile, or by means of Internet access, Internet e-mail or Internet telephony. By virtue of the definition of the concept of data set out in section 1 (see preceding paragraph), the Act is exclusively concerned with transactional information affecting such matters as the location and identity of subscribers and users of communications devices; its provisions accordingly do not affect the content of communications.

78. Section 3 imposes the obligation on a Service Provider to collate and retain data relating to electronic communications of the kind specified in Schedule 2 of the Act (set out in detail below at paragraphs 81-82).

79. Such data is to be retained in a manner that facilitates prompt disclosure when requested by a body or person authorised to make such a request.

80. Section 3 also makes provision for the periods for which retained data must be stored by Service Providers – viz., two years in respect of data on communications made by telephone, fixed or mobile, and one year for data connected with Internet access, Internet e-mail and Internet telephony.

Retained Telephony Data

81. Part 1 of Schedule 2 sets out the types of fixed network telephony and mobile telephony data that must be retained under section 3 of the Act as follows:

> *"Fixed network telephony and mobile telephony data to be retained under section 3*
>
> *1. Data necessary to trace and identify the source of a communication:*
>
> *(a) the calling telephone number;*
>
> *(b) the name and address of the subscriber or registered user.*
>
> *2. Data necessary to identify the destination of a communication:*
>
> *(a) the number dialed (the telephone number called) and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;*
>
> *(b) the name and address of the subscriber or registered user.*
>
> *3. Data necessary to identify the date and time of the start and end of a communication.*
>
> *4. Data necessary to identify the type of communication:*
>
> *the telephone service used.*
>
> *5. Data necessary to identify users' communications equipment or what purports to be their equipment:*
>
> *(a) the calling and called telephone number;*
>
> *(b) the International Mobile Subscriber Identifier (IMSI) of the called and calling parties (mobile telephony only);*

(c) the International Mobile Equipment Identity (IMEI) of the called and calling parties (mobile telephony only);

(d) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated (mobile telephony only).

6. Data necessary (mobile telephony only) to identify the location of mobile communication equipment:

(a) the cell ID at the start of the communication;

(b) data identifying the geographical location of cells by reference to their cell ID during the period for which communication data are retained."

Retained Internet Data

82. The types of data that must be retained in respect of Internet communications are set out in Part 2 of Schedule 2 of the Act:

"Internet access, Internet e-mail and Internet telephony data to be retained under section 3

1. Data necessary to trace and identify the source of a communication:

(a) the user ID allocated;

(b) the user ID and telephone number allocated to any communication entering the public telephone network;

(c) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

2. Data necessary to identify the destination of a communication:

(a) the user ID or telephone number of the intended recipient of an Internet telephony call;

(b) the name and address of the subscriber or registered user and user ID of the intended recipient of the communication.

3. Data necessary to identify the date, time and duration of a communication:

(a) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access Service Provider to a communication, and the user ID of the subscriber or registered user;

(b) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.

4. Data necessary to identify the type of communication:

the Internet service used.

5. Data necessary to identify users' communication equipment or what purports to be their equipment:

(a) the calling telephone number for dial-up access;

(b) the digital subscriber line (DSL) or other end point of the originator of the communication.

Security of Retained Data

83. In light of its extensive data retention provisions, and having regard to the vast corpus of information touching the private lives of a huge swathe of the population placed in the

hands of Service Providers as a result of its operation, the 2011 Act requires custodians of retained data to take appropriate security measures in respect of the storage and disclosure of such data. Thus section 4(1)(b) provides that once a database has been established it "shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure."

84. The obligation thus imposed on Service Providers by section 4 follows the wording of Article 7 of Directive 2006/24/EC (to which the 2011 Act is intended to give effect). It will be seen in due course that one of the grounds upon which the ECJ in *Digital Rights Ireland* declared this Directive void was the inadequacy of its data security provisions; broadly speaking, they were considered to be too general and insufficiently prescriptive. It should also be noted that section 4 of the 2011 Act is silent on the issue of breach of security, notwithstanding that it specifically contemplates the possibility of unlawful as well as merely accidental interference with retained data. Neither is there any sanction provided for in case of a failure by a Service Provider to comply with section 4.

85. Section 4 also provides for the destruction of data by the Service Providers once the statutory period for retention has expired – viz., two years in respect of telephone communications data and one year in respect of Internet communications data. The obligation is to destroy all retained data within one month of the expiry of the applicable statutory retention period.

86. Thus It follows that at any given moment there is a corpus of retained communications data spanning the immediately preceding two years, in the case of telephony data, and one year in the case of Internet data, which, given the rolling deletion dates enshrined in section 4, may extend to data covering the previous 25 and 13 months, respectively.

87. It should be noted that the obligation placed on Service Providers to destroy data on the expiry of the relevant statutory period does not apply to data which have been accessed pursuant to a disclosure request under section 6. Such data may be retained both by the

requesting authority and by the Service Provider. Data thus retained by a Service Provider is referred to as a ''golden copy''. While it is perfectly understandable that Service Providers retain a ''golden copy'' of disclosed data for the purpose of giving evidence in court proceedings, it is striking that section 4 makes no provision for destruction when there is no further need for retention for this or any other lawful purpose.

88. Finally, section 4(2) - which designates the Data Protection Commissioner "as the national supervisory authority for the purposes of this Act and Directive No. 2006/24/EC of the European Parliament and of the Council" - might be thought to have a bearing on the issue of data security. However, the section says nothing about how ''the national supervisory authority'' might exercise any powers in this regard, what these powers might be or how often they should be exercised. Article 9 of Directive 2006/24/EC states that the supervisory authority is responsible for monitoring the security of stored data. In essence, this seems to mean that the Data Protection Commissioner must ensure that Service Providers comply with their obligations under Section 4(1)(a)-(b) – set out above at paragraphs 83-85.

Access to Retained Data

89. Section 5 of the Act expressly prohibits Service Providers from accessing retained data except:

> *"(a) at the request and with the consent of a person to whom the data relate,*
>
> *(b) for the purpose of complying with a disclosure request,*
>
> *(c) in accordance with a court order, or*
>
> *(d) as may be authorised by the Data Protection Commissioner."* [Emphasis added]

90. The disclosure requests provision is the most frequently used of the exceptions listed in section 5. Disclosure requests must be made in accordance with the provisions of section 6. Disclosures relate in the main to requests made by the Garda Síochána and the

Permanent Defence Force; and less frequently to requests from GSOC and the Revenue Commissioners. The Competition and Consumer Protection Commission informed the Review that it had not, so far, availed of the section 6 procedure.

91. Disclosure requests under section 5(a) – requests made by the person to whom the data relate – though not unusual, appear to be small in number. Typically, the request is made in person or through a solicitor who is required to show his or her client's consent in writing. The provision is not without its ambiguities such as whether a person who receives a communication, in addition to the person who initiates it, comes within its ambit. Any other person probably falls outside the ambit of the provision, even if it could be said that the data 'relate' to them in some other way.

92. The exception in section 5(c) is important even if a court might not in all circumstances, or perhaps in any circumstances, be characterised as a statutory body; albeit that the functions of a judge of the District Court under the provisions of the Criminal Justice (Mutual Assistance) Act, 2008 when he or she is acting as a designated judge for the purposes of that Act, at least warrants special scrutiny in this regard. The disclosure of personal information on foot of a court order made pursuant to section 5(c) could have serious ramifications for journalists; as already indicated, retained communication data on the pattern of a journalist's contacts over an extended period may have a clear bearing on the identification of his or her sources.

93. Finally, section 5(d) refers to access authorised by the Data Protection Commissioner. The Review has been informed by the Data Protection Commissioner that no authorisation has ever been issued under Section 5(d); and this was confirmed by the Service Providers consulted by the Review.

Accessing Bodies

94. As already indicated, section 6 identifies, inter alia, the statutory bodies entitled to make a disclosure request; viz.,

- the Garda Síochána;
- the Permanent Defence Force;
- the Revenue Commissioners;
- the Competition and Consumer Protection Commission.
- Section 6(1) provides that a member of the Garda Síochána not below the rank of Chief Superintendent may make a disclosure request to a Service Provider where he or she is satisfied that the data are required for:

> *"(a) the prevention, detection, investigation or prosecution of a serious offence,*
>
> (b) *the safeguarding of the security of the State,*
>
> *(c) the saving of human life."*

95. As already indicated, Garda access to retained data is also permitted under section 8(b) of the Data Protection Acts 1988 and 2003, as amended. Moreover, access under section 8(b) is not confined to data relating to serious offences; it is enough that the requested data is ''required for the purpose of preventing, detecting or investigating *offences''* (emphasis added).

96. Similarly, section 6(2) provides that an officer of the Defence Force not below the rank of Colonel may make a disclosure request for data concerning any person "where that officer is satisfied that the data are required for the purpose of safeguarding the security of the State".

97. Penultimately, section 6(3) authorises an officer of the Revenue Commissioners not below the rank of Principal Officer to make a disclosure request "where that officer is satisfied that the data are required for the prevention, detection, investigation or prosecution of a

revenue offence." A revenue offence is defined in section 1 of the Act as "any offence under any of the following provisions that is a serious offence"; while the term serious offence is itself defined as one punishable by imprisonment for a term of five years or more. The ''following provisions'' referred to are contained in the Customs Consolidation Act, 1876, the Taxes Consolidation Act, 1997 and various Finance Acts, respectively. It is not necessary for present purpose to recite in detail the wide range of offences covered by these provisions. Suffice it to say that the offences in respect of which an officer of the Revenue Commissioners may make a disclosure request pursuant to section 6 are confined to those offences in the specified sections which are punishable by imprisonment for a term of five years or more. It should however be noted that some of these offences are not serious offences in the relevant sense if prosecuted summarily; this is because the associated penalty of 5 years' imprisonment arises only on conviction on indictment.

98. Finally, it should be noted that the scope of section 3 has been widened by the inclusion of a new provision covering data access requests by the Competition and Consumer Protection Commission, a body established by the Competition and Consumer Protection Act, 2014. Thus the new section 6(3A), as inserted by section 89(b)(1) of the 2014 Act, provides as follows:

> *''A member of the Competition and Consumer Protection Commission may request a Service Provider to disclose to that member data retained by the Service Provider in accordance with section 3 where that member is satisfied that the data are required for the prevention, detection, investigation or prosecution* of a competition offence.''

99. A ''competition offence'' is described in an amendment to section 1 (the Interpretation section) of the 2011 Act as:

''an offence under section 6 of the Competition Act 2002, that is an offence involving an agreement, decision or concerted practice to which subsection (2) of that section applies.''

100. It will be seen that there is no requirement that a competition offence must be a serious offence. By virtue of section 8(1) of the Competition Act 2002, a section 6 offence can be prosecuted either summarily or on indictment. By definition, if prosecuted summarily a section 6 offence is not a serious offence by reference to the definition in the 2011 Act. Moreover, if prosecuted on indictment, section 6 offences carry a maximum penalty of five years' imprisonment, and thus appear to come within the criterion of seriousness laid down in section 1 of the 2011 Act. In addition, since section 6 offences prosecuted on indictment may also be punished by fines running to several million Euro or ten percent of turnover, whichever is the greater, and bearing in mind that the issue of imprisonment will not normally arise in the case of corporate undertakings, the Review is satisfied that they should be treated as serious offences in such cases and that the Interpretation section of the 2011 Act, or any Act amending or replacing it, should be adjusted accordingly.

101. The Garda Síochána Ombudsman Commission relies on section 98(1) and (2)(c) of the Garda Síochána Act, 2005 when making a request for access to data pursuant to section 6. Section 98(1) provides that if directed by the Ombudsman Commission "to investigate a complaint under the section, a designated officer has ... for the purposes of the investigation all powers, immunities and privileges conferred and all duties imposed on any member of the Garda Síochána by or under any enactment ..."

102. Section 98 (2)(c) provides that, for the purposes of subsection (1),

"An enactment conferring a power, immunity or privilege or imposing a duty on a member of the Garda Síochána in relation to any of the matters specified in that subsection applies with the following modification and any other necessary modifications:

` *"(c) a reference in the enactment to a member of the Garda Síochána not below `the rank of inspector is to be read as a reference to a member of the Ombudsman Commission."*

103. GSOC has confirmed to the Review that disclosure requests pursuant to section 6 are routinely made on the basis of the scheme set out in the immediately preceding paragraphs.

104. By virtue of section 6(4)-(5) all disclosure requests must be made in writing but may be made orally in cases of exceptional urgency. If made orally, the request must be confirmed in writing within two working days.

105. Service Providers are obliged by section 7 to comply with a disclosure request; but the Act makes no provision in the event of failure or refusal to comply.

Limiting Grounds of Access

106. Section 6 seeks to limit the power of access by linking it to specific purposes (following the provisions of Article 15(1) of Directive 2002/58). Thus access by the Garda Síochána under section 6(1)(a) is exclusively for the purposes of combating serious crime, safeguarding the security of the state, and saving human life. Some of these criteria – safeguarding the security of the state, for example - are less tightly drawn than others. The insider trading and market manipulation offences under Regulation 5 and 7 of the European Union (Market Abuse) Regulations 2016 which are deemed to be serious via their insertion into Schedule 1 to the 2011 Act, do not of themselves meet the seriousness criterion of carrying a penalty of imprisonment of five years or more as laid down in section 1 of the Act. While these offences attract a potential fine of €500,000, a maximum imprisonment penalty of three years applies to them. These differences and discrepancies, together with the difficulty of framing uniform limits when circumscribing the power of access to retained data are discussed in detail later.

107. Section 8 of the Data Protection Acts 1988 and 2003, as amended, is especially significant in this regard. In particular, section 8(b) provides for the disapplication of restrictions on disclosure of personal data where disclosure is:

> *''Required for the purpose of preventing, detecting and investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other monies owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid.''*

108. The Review has learned that a composite procedure involving section 8(b) and section 6 of the 2011 Act had been relied upon by the Garda Síochána when making requests to Service Providers for retained communications data. Following an audit by the Data Protection Commissioner of Garda practice in this area in 2014, this arrangement was modified such that section 8(b) is currently invoked only in respect of requests pertaining to non-serious offences – in other words, requests that fall outside the scope of the 2011 Act. Suffice it to say at this juncture that it is anomalous that section 8(b) was not repealed (or at least amended) with the introduction of the 2011 Act. Broadly speaking, section 6(1)(a) of the 2011 Act confines disclosure requests by the Garda Síochána to the investigation of serious crime, whereas the section 8 procedure recognises no such limitation as it is available in respect of criminal offences generally. Moreover, as will be discussed later, the criteria governing the management of private communications data held by Service Providers must now be seen through the prism of the decision of the ECJ in *Tele2*which expressly limits both the retention and disclosure of such data to purposes directly connected with the prevention of serious crime.

109. As already indicated, section 8(b) permits access to personal data including retained communications data for a variety of purposes, including the collection of monies owed to the state, a local authority or a health board. The section also permits access to such data for the purpose of investigating minor offences and has been so used by the Garda Siochana. As explained in detail in Chapter 2, retained communications data may only be

accessed for the purposes envisaged by Article 15(1) of Directive 2002/58/EC. In the field of criminal investigation access may be sought in connection with serious offences only. Access to retained data for the other purposes mentioned above is precluded by EU law since they fall outside the purposes covered by Article 15(1). Moreover, the access provided for in section 8(b) is not made subject to the safeguards necessary under EU law or arising from obligations under the ECHR intended to ensure compliance with the principle of proportionality. Accordingly, having regard to the fact that section 8 of the Data Protection Acts 1988-2003 permits acess to retained communications data in circumstances and for purposes precluded by EU law, it is recommended that the section be repealed or at least disapplied in the matter of access to retained communications data. (**R**)

Reporting System

110. Section 9 makes provision for the preparation and submission of an annual report by the various data accessing bodies to their respective ministers in respect of all disclosure requests made under section 6(3) during the relevant period. By virtue of section 9(5), these reports are required to include:

> *"(a) the number of times when data has been disclosed in response to a disclosure request,*
>
> *(b) the number of times when a disclosure request could not be met,*
>
> *(c) the average period of time between date when data were first processed and the disclosure request."*

111. The Minister for Defence, the Minister for Finance, and the Minister for Jobs, Enterprise and Innovation are required to forward to the Minister for Justice the respective reports received by them, together with any comments they may have on them.

112. On the basis of these reports and the report received from the Garda Síochána, a consolidated report is then prepared by the Minister for Justice for submission to the European Commission.

Complaints Procedure

113. Section 10 of the Act provides for a complaints procedure where there is a contravention of section 6 in relation to a disclosure request. Any such contravention is subject to an investigation in accordance with the provisions of section 10. It should be noted that section 10 provides that a contravention of section 6 shall not of itself render the disclosure request invalid or constitute a cause of action at the suit of a person affected by the disclosure request. However, section 10 expressly provides that it does not affect a cause of action for the infringement of a constitutional right.

114. The complaints procedure can only be triggered by an application from a person who believes that data relating to him or her are in the possession of a Service Provider and have been accessed following a disclosure request. That person may then apply to the Complaints Referee for an investigation into the matter. It should be noted that this procedure is confined to applicants who believe their private data has been accessed, and thus presumably is not open to the simply curious or merely suspicious in this regard. On the other hand, in many or most cases a journalist or any person would have no means of knowing that their private data had been accessed and thus would not be in a position to lodge a complaint.

115. Save where it is deemed frivolous or vexatious, the Referee is obliged by Section 10(3) to determine whether a disclosure request was made as alleged in the application and if so, whether any provision of section 6 – governing the conditions and forms of disclosure requests - has been contravened.

116. If it is found that the provisions of section 6 have been contravened, the Referee is bound to notify the application "of that conclusion" and "make a report of the Referee's findings to the Taoiseach". Only the conclusion is notified to the applicant.

117. Where a contravention of section 6 has been found, Section 10(5) gives additional powers to the Referee, to be exercised only if he or she thinks fit, to make orders (a) directing the destruction of retained data and (b) recommending the payment of compensation to the applicant. The decision of the Referee under the section is final; and the Minister is obliged to implement any recommendation in respect of compensation.

Designated Judge

118. Sections 11 and 12 contain important provisions on the role and functions of a "designated judge" charged with reviewing the operation of the Act, the compliance of the relevant statutory bodies with its provisions, and the preparation and submission of reports to the Taoiseach.

119. Section 11 amends section 8 of the Interception of Postal Packets and Communications Messages (Regulation) Act, 1993 so as to provide that the judge designated for the purpose of the 1993 Act is also a Designated Judge for the purposes of the 2011 Act.

120. For the purposes of carrying out his or her duties, the designated judge has power to investigate any matter and access official documents or records relating to a particular disclosure request, and may communicate with the Taoiseach or the Minister as he or she sees fit.

121. The limited nature of the review procedures contemplated by these provisions, particularly in light of the ruling in this regard in *Tele2,* will be referred to later.

Garda Síochána Ombudsman Commission and the Garda Síochána Act, 2005

122. As already indicated, given that they are taken to provide the basis on which GSOC makes disclosure requests pursuant to section 6 of the 2011 Act, section 98(1) and (2)(c) of the Garda Síochána Act, 2005 form an important part of the statutory framework at issue in this Review. Leaving aside any question concerning the validity of GSOC's interpretation of section 98 of the 2005 Act in this regard, one of the key recommendations in the Review is that the rules (and powers) governing access to retained data should be explicitly stated and contained in a single enactment, and that changes thereto, whether by way of addition or modification, should be incorporated as amendments to that enactment. Apart from the issue of the fragmentation of pertinent sources of law by locating them in different enactments, GSOC's reliance on section 98 as a basis for making disclosure requests means that it does not appear to be bound by key sections of the principal enactment in the area. Thus GSOC does not appear to be bound by section 9 of the 2011 Act – which requires the requesting bodies mentioned in the Act to submit written reports of their activities to a designated minister.

123. By parity of reasoning, the oversight function assigned to a designated judge by the 2011 Act does not appear to cover GSOC; section 12(1)(b) seems to confine the former to the Garda Síochána, the Defence Force, the Revenue Commissioners, and the Competition and Consumer Protection Commission. At best it may be said that the designated judge has some implicit functions insofar as he or she has a duty to keep the operation of the Act under review and the power to investigate any case in which a disclosure request is made. In this regard, the Review is aware that the designated judge has in practice routinely included GSOC in his review of the operation of the 2011 Act. Nonetheless, it is not entirely satisfactory that the powers of the designated judge in this matter are not expressly stated in the enactment setting them out. By the same token, it is less than satisfactory that GSOC itself is not mentioned in the principal enactment governing access to retained communications data, and thus made expressly subject to its provisions and safeguards.

Criminal Justice (Mutual Assistance) Act, 2008

124. The Criminal Justice (Mutual Assistance) Act, 2008 (hereinafter the 2008Act) is also part of the legislative framework governing access to retained data held by Service Providers. As its long title makes clear, the purpose of the 2008 Act is, *inter alia*, to give effect to certain international agreements between the state and other states relating to mutual assistance in criminal matters. While the 2008 Act makes no reference to retained communications data as such, section 75 of the Act provides an avenue of access to retained data for the purpose of complying with a request by a foreign police or security agency. Thus a member of the Garda Síochána not below the rank of inspector, on the direction of the Minister for Justice, may apply to a designated judge of the District Court for an order requiring a Service Provider to furnish retained data in respect of a particular person over a specified period. Once the procedures governing application to the District Court have been complied with, the judge in effect has no discretion to refuse the application. Moreover, by virtue of section 5 of the 2011 Act, Service Providers in turn are required to grant access to retained data in accordance with a court order thus obtained.

125. It has not been possible to put a definitive figure on the number of requests which have up to now been made pursuant to section 75 of the 2008 Act. The best estimate is that the overall number is approximately 250 per year, although the Review has been told that the annual number is steadily increasing.

126. The principle of mutual assistance at the core of the 2008 Act implies reciprocal and broadly equivalent arrangements between law enforcement agencies in respect of the generation and exchange of evidential material in connection with the detection and prosecution of crime. In the specific context of telecommunication data, this element of reciprocal equivalency may be said to be something of a misnomer. As matters stand, some of the countries entitled to seek the private data of individuals held in this country would not be in a position to reciprocate a similar request from this country, either because they do not have a communications data retention regime at all or because their data retention time limits are significantly shorter than those obtaining in Ireland. It

should also be borne in mind in this connection that the respective international and domestic data access regimes in the 2008 and 2011 Acts are not co-extensive. For example, section 75 countenances foreign requests in respect of persons suspected of offences punishable by a term of six months' imprisonment, whereas, as seen above, the 2011 Act sets the domestic threshold in this matter at offences carrying a minimum of five years' imprisonment. This is wholly incompatible with the principle that access to retained data may only occur in respect of serious criminal offences.

127. None of this is intended to detract from the imperative need for active and extensive cooperation between the policing authorities of different countries, especially in an age of organised transnational terrorism. The point is rather to emphasise that international cooperation in criminal matters should be consistent with constitutional norms and EU law, including the general principle of proportionality. Accordingly, in the sphere of immediate concern to this Review – access to retained communication data, and, in particular, the communications data of journalists – the key issues to be addressed are the appropriateness of the criteria governing foreign requests for access to private data of this kind, as well as the adequacy of the safeguards surrounding the proper use of private data by foreign authorities.

128. As already indicated, access to private data for the purpose of complying with a foreign request is normally processed by means of the procedure laid down in section 75 of the 2008 Act: the original request is sent to the Minister for Justice who is the central authority for mutual assistance in criminal matters under the Act; the Minister then instructs a member of the Garda Síochána not below the rank of inspector to apply to a judge of the District Court for an order directing the Service Providers to release the relevant data.

129. The Department of Justice has informed the Review that other means of obtaining evidence may also be employed under the rubric of section 75. For example, the requested evidence could be obtained on foot of a search warrant; this procedure might be used where the entity holding the evidence was deemed to be hostile, or where there was

a concern that the subject of the investigation might destroy the evidence. Alternatively, evidence might be secured by issuing a subpoena to a company representative requiring them to appear before a nominated judge of the Dublin District Court and compelling them to bring relevant documentation to court.

130. Apparently the decision as to which procedure to use is made at an administrative level within the Department. Unless there are specific reasons for deviating from it, requests for specified evidential material held by data Service Providers are usually processed by following the standard procedure laid down by section 75. The range of offences comprehended by foreign requests is extensive. Evidence supplied pursuant to section 75 can only be used for the purpose for which it is sought. The 2008 Act also provides for the repatriation of evidence following the conclusion of criminal proceedings, but in practice the return of evidence is rarely sought.

131. Detailed commentary on the provisions of the 2008 Act is beyond the scope of this Review. Suffice it to say for present purposes that there are no meaningful *de minimis* requirements in the Act - or for that matter in the administrative scheme operated by the Department of Justice - regarding the seriousness of offences in respect of which retained data access requests can be made and executed. This contrasts sharply with several jurisdictions which have thresholds well in excess of the Act's baseline of offences carrying terms of imprisonment of 6 months. As already indicated, it also stands in stark contrast with the threshold specified in the 2011 Act which is largely confined to serious offences carrying a minimum of 5 years' imprisonment.

132. As can be readily seen, the purpose and objectives of the 2008 Act are fundamentally different from those of the 2011 Act. In the present context, the former is concerned with providing evidence and information, including communications data, to authorities outside the state for use outside the state in accordance with certain international conventions and EU Decisions; whereas the latter is concerned with providing access to communications data to specified authorities within the state for use within the State.

133. The key issue for the Review is that the 2008 Act provides a means of – albeit indirect - access to retained communications data, including the communications data of journalists, by foreign authorities. Although this data is retained by Service Providers pursuant to their obligations under the 2011 Act, there is no express provision in that Act for access to such data by or for the benefit of foreign authorities. Accordingly, as an absolute minimum, the Review is of the opinion that access to retained data of the kind facilitated by the 2008 Act should be subject to the normal criteria governing access by statutory bodies, not only as currently laid down in the 2011 Act but in any amending legislation. Moreover, access to retained communications data should be governed by and accord with appropriate safeguards for the protection of fundamental rights and freedoms. These safeguards -discussed in detail in Chapter 3 - derive principally from those identified by the ECJ in *Tele2*and the State's obligations under the European Convention on Human Rights.

CHAPTER TWO: FUNDAMENTAL RIGHTS DIMENSION

UNDER EU LAW

Preamble

134. It is now accepted that the compulsory retention of private communications data, particularly when applied indiscriminately and comprehensively to the electronic communications of all persons within the State, involves a serious infringement or curtailment of nationally and internationally recognised fundamental rights. This is not to suggest that a state cannot engage in any form of broad communications data retention forthe purposes of combating serious crime or terrorism or similar purposes. The key concern of national constitutional courts, international courts and international fora has been on the need to ensure that a statutory data retention scheme established for this purpose pays due regard to the principle of proportionality: in other words, without putting the issue of the scope of the scheme in question, with ensuring that interference with fundamental rights is confined to what is strictly necessary for the achievement of legitimate public interest objectives.

135. Accordingly, constitutional courts in countries as far apart as Mexico and Romania have condemned, and in many instances, struck down statutory regimes based on the principle of mass, indiscriminate retention of electronic communications data. The principal criticism has been that, in the absence of appropriate safeguards, a statutory regime of this nature fails to strike an appropriate balance between promoting public interest objectives and safeguarding human rights. A more fundamental criticism came to the fore in the recent decision of the ECJ in the *Tele2*: namely, that a system of indiscriminate data retention is so broadly based that it must be considered incompatible with applicable EU law as interpreted in the light of express guarantees in the Charter of Fundamental Rights of the European Union. On this reasoning, set out at paragraph 112 of the judgment in that case, the system's the lack of proportionality cannot be cured by

adding safeguards and procedures for the protection of fundamental rights since the unlimited scope of the system in and of itself constitutes a serious interference with those rights. In other words, because the system itself is inherently unlawful.

136. In the result, the permissible limits of data retention and disclosure must now be gauged primarily through the prism of EU law interpreted in light of the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union: principally, though not exclusively, the rights to privacy, the protection of personal data, and freedom of expression, respectively. In addition, when seeking to determine these limits, regard must also be had to the concurrent obligations of the State in respect of the fundamental rights guaranteed and protected by the European Convention on Human Rights (ECHR).As will be seen in due course, the decisions of the European Court of Human Rights in the areas of privacy and freedom of expression have particular relevance to this undertaking. Taken together these two sources of law have had a seminal influence on the principles, policies and standards that must now be reflected in domestic legislation purporting to establish a viable system of data retention and disclosure.

Rights at Issue

137. The Charter rights identified in the case law of the ECJ as endangered by a system of automatic and indiscriminate data retention are as follows:

- Respect for private life, guaranteed by Article 7: “Everyone has the right to respect for his or her private … life … and communications.”

- Protection of personal data, guaranteed by Article 8:”Everyone has the right to the protection of personal data concerning him or her. Rules governing protection of this right shall be subject to control by an independent authority.”

- Freedom of expression and information, guaranteed by Article 11: "Everyone has the right to freedom of expression. This includes freedom to receive and impart information without interference by public authority. The freedom … of the media shall be respected."

Primacy of EU Law

138. Before outlining the jurisprudence of the ECJ on the decisive role played by the aforementioned Charter rights in the matter of data retention and disclosure, and its implications for domestic legislation in the area, the principle of the primacy of the law of the European Union over domestic law, including constitutional law, deserves to be noticed.

139. This is a well-established principle incorporated by amendment to Article 29.6 of the Constitution which states: "No provision of this Constitution invalidates laws enacted, Acts done or measures adopted by the State, … that are necessitated by the obligations of membership of the European Union … ". The primacy principle means that EU law is embedded in the national legal systems of Member States so as to constitute an autonomous source of law which takes precedence over purely domestic law. Accordingly, it follows that an assessment of the proper limits of any given piece of national legislation must include a concomitant assessment of the extent to which the subject matter has been affected by European law.

140. The case of *Schrems v Data Protection Commissioner*[21] provides an example of the primacy of EU law and the latter's relationship in these circumstances with national

[21] [2014] 3 IR 75

constitutional protections. The issue in that case was the validity of a decision of the Data Protection Commissioner under the Data Protection Acts, 1988 – 2003 giving effect, inter alia, to Commission Decision 2000/520 whereby personal data was permitted to be transferred by "Facebook" for storage in servers in the USA and thus accessible by US agencies under US law. It was contended that a foreign transfer of this kind was incompatible with the protection of the fundamental rights of citizens in this country. Having been raised before the High Court, this issue was made the subject of a reference to the Court of Justice. The ECJ summarised the High Court's position as regards the protection of constitutional rights under the Constitution of Ireland as follows (at paragraph 33 of its Judgment):

> *"The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or group of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of serious doubt as to whether the United States ensures an adequate level of protection of personal data, ... the Commissioner was wrong in rejecting the complaint."*[22]

141. However, the High Court concluded that since the matter at issue was governed by EU law the legality of the data transfer at the centre of the proceedings could only be

[22]Case C-362/14

assessed in the light of EU law and not solely by reference to the Constitution. (in the event, the ECJ found, *inter alia*, that Commission Decision 2006/24 was invalid in failing to respect certain fundamental rights guaranteed by the Charter of Fundamental Rights.)

142. The protection of fundamental rights in Ireland involves the complex interrelationship between constitutional protections, protections contained in EU higher norms such as the Treaties and the Charter, the European Convention on Human Rights (to which the State is a party), and national and EU legislation. Where issues concerning the protection of fundamental human rights are governed by EU law, the primacy of the latter means that the protection given to such rights by the provisions of the Constitution are not strictly pertinent.

143. As mentioned in the preceding paragraph, the State has a concurrent obligation, at international level, to ensure the protection of similar or corresponding rights guaranteed by the European Convention on Human Rights (ECHR). However, the protection of rights under the ECHR in accordance with the jurisprudence of the European Court of Human Rights, while creating binding obligations on the State, does not take precedence over constitutional protections or domestic legislation in the manner of EU law. There is, nonetheless, an important relationship between the rights guaranteed by EU law and, in particular, by the Charter and those guaranteed under the European Convention. Article 52 of the EU Charter of Fundamental Rights provides:

> *"Insofar as this Charter contains rights which correspond to the rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."*

144. Although there is potential for divergence between obligations arising under EU law, on the one hand, and the ECHR, on the other, this possibility is more theoretical than real in the present context since the essence of the rights at issue in the matter of data retention and disclosure are similar in both legal settings, as are the accompanying

safeguards identified in the complementary case law of the ECJ and the ECtHR. Indeed, the two courts from time to time make reference to each other's case law on data retention and disclosure. That said, as will be seen presently, EU law has set strict limits to the scope of data retention systems, whereas the ECtHR has not addressed this issue.

145. Thus both EU law and the law of the ECHR have direct relevance for the formulation of policy and consequential legislation at national level as to the form and scope of any legislation imposing an obligation on Service Providers to retain communications data. The same applies to the balance to be struck between the perceived need for a system of data retention and the protection of the fundamental rights necessarily affected by its operation. In both instances, the starting point for legal analysis is a comprehensive assessment of the applicability of EU law, including the rights guaranteed under it, to any legislative scheme purporting to sanction the retention and disclosure of communications data.

146. The Communications (Retention of Data) Act, 2011 was adopted with a view to fulfilling the State's obligation to give effect to EU Directive 2006/24/EC on the retention of data related to electronic communication services. That Directive sought, *inter alia*, to harmonise the obligations imposed on Member States in the matter of data retention and disclosure. Accordingly, the system of data retention established by the 2011 Act is in essence the system provided for in Directive 2006/24. Most of the substantive provisions of the 2011 Act adopt or follow the wording of the Directive. Thus – to cite a single example - the core provisions of the Directive setting out the precise nature and scope of the telephone and internet data to be retained are repeated almost verbatim in Schedule 2 of the Act.

147. The compatibility of Directive 2006/24 with EU law was scrutinised by the ECJ for the first time in 2014 in *Digital Rights Ireland*.[23]In that case the Directive was declared invalid on the grounds that the system of communications data retention which it established constituted a serious and disproportionate interference with certain fundamental rights and freedoms guaranteed by the EU Charter of Fundamental Rights. The Court concluded that the Directive must be regarded as breaching the principle of proportionality as it failed to provide for adequate accompanying safeguards forthe protection of the fundamental rights affected by the retention of communications data system enshrined in it. It did not, however, decide that the data retention system *per se* was incompatible with EU law.[24]Rather it sought to lay down a set of standards and benchmarks for the kind of safeguards EU law regarded as essential for compliance with the principle of proportionality in the matter of data retention.

148. In the event, this approach has been overtaken by the recent judgment of the Court on 21 December, 2016 in*Tele2*,[25]even if its influence on the reasoning in the latter case is evident. The judgment in *Digital Rights Ireland* included a finding that a general system of communications data retention as envisaged in Directive 2006/24 directly interfered "*in a particularly serious manner*" with fundamental rights to respect for private life and the protection of personal data. The Court also found that data retained and subsequently used without the subscriber or registered user being informed of the fact, is likely to generate in the persons affected a feeling that their private lives are the subject of

---

[23]8th April, 2014: Joined cases C-293/12 and C-594/12 – the judgment pronounced on these issues of law arising from two references by respectively the High Court of Ireland and the Constitutional Court of Austria, pursuant to Article 267 TFEU.

[24]In contrast to the subsequent decision of the Court in the *Tele2* case as regards such an indiscriminate and generalised retention of communications data.

[25] Joined cases C-203/15 and C-698/15 being respectively references to the ECJ pursuant to Article 267 by the Administrative Court of Appeal, Stockholm, Sweden and the Court of Appeal (Civil Division) of England and Wales.

constant surveillance. In declaring the Directive invalid, the Court found, inter alia, that Article 4 of the Directive did not expressly provide that access and subsequent use of the data in question "*must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto;[rather] it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements*."

149. In short, the Directive was declared invalid because it was deficient on the measures and procedures that should have been included in order to uphold the principle of proportionality and protect fundamental rights. The decision did not however pronounce on the validity of national legislation purporting to give effect to the Directive, or otherwise providing for communications data retention. Nor did it pronounce directly on the extent to which EU law applied to national legislation of this nature, or on the important question of access by national authorities to retained communications under such legislation.

150. Indeed the ECJ in*Tele2* noted in this connection that the parties in that case (including government parties) disagreed on the scope of the judgment in *Digital Rights Ireland* and its effect on national legislation.

Key Issues in *Tele2*

151. Although the judgment in *Digital Rights Ireland* was pregnant with implications for the validity of national legislation which established the kind of data retention regime enshrined in Directive 2006/24, these implications were not spelled out and did not form part of the conclusions in that case. In the result, national legislation which had given effect to Directive 2006/24 continued in force in most Member States (Germany, the Netherlands and Belgium are among the exceptions.) It is not surprising, therefore, that the question of the validity of national legislation enacted to give effect to Directive 2006/24 was eventually referred to the ECJ. This happened by way of references by courts in Sweden

and England and Wales made pursuant to Article 267 of the Treaty on the Functioning of the European Union (TFEU). The judgment in these joined cases was given by the ECJ in *Tele2*.[26] In its reference the Swedish Court of Appeal requested, *inter alia*:

> *"that the Court give an unequivocal ruling on whether, … the general and indiscriminate retention of electronic communications data is per se incompatible with Articles 7 and 8 and Article 52(1) of the Charter, or whether, the compatibility of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention".*

152. For its part, the Court of Appeal of England and Wales asked whether the Court's judgment in *Digital Rights Ireland* laid down:

> *"mandatory requirements of EU law applicable to a Member State's domestic regime concerning access to data retained in accordance with national legislation in order to comply with Articles 7 and 8 of the Charter."*

Impugned Enactment

153. In *Tele2* the ECJ frequently refers to the kind of legislation under scrutiny by the court as legislation "such as that in the main proceedings". This in turn refers to the national legislation on communications data retention in Sweden and England and Wales in respect of which the aforementioned courts in these countries made their references to the ECJ. Referring specifically to the Swedish legislation, the ECJ described it, at paragraph 97 of the Judgment, as an enactment which "provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communications, and that imposes on providers of electronic

[26] See footnote 2 above

communications services an obligation to retain that data systematically and continuously with no exceptions." The ECJ also pointed out that the Swedish legislation was enacted for the specific purpose of giving effect to Directive 2006/24, later declared invalid by the Court.

154. This brings us directly to the Communications (Retention of Data) Act, 2011 which forms the core of the Irish legislative framework referred to in the Terms of Reference of this Review. As the Court pointed out, the categories of data required to be retained by the Swedish legislation correspond, in essence, to those enshrined in the data retention regime set out in Directive 2006/24; and as the reader will have noticed, the latter is virtually on all fours with the data retention scheme Service Providers in Ireland are obliged to maintain pursuant to their obligation under the 2011 Act. In a word, the Communications (Retention of Data) Act, 2011 falls squarely into the category of the kind legislation under scrutiny in *Tele2*; and, like its Swedish counterpart, was enacted to give effect to Directive 2006/24 EC. In the result, it goes without saying that the judgment in *Tele2*is of capital importance when assessing the compliance of the 2011 Act with applicable EU law and standards in the matter of data retention and disclosure, and, in particular, with the safeguards for fundamental rights essential to the proper regulation of this area; and that such an assessment is a key component of any policy evaluation of the Act.

Principle of Confidentiality

155. The ECJ first examined whether national legislation of the kind described in the penultimate paragraph fell within the scope of EU law and, in particular, that of Directive 2002/58 (Directive on Privacy and Electronic Communications). The Court referred, inter alia, to Article 5 of that Directive, headed "Confidentiality of Communications" and noted that it was designed to ensure the confidentiality of communications and related traffic data. In particular, Article 5 prohibited listening, tapping, storage or other kinds of interception or surveillance of communications except when legally authorised in accordance with Article 15(1) of the Directive.

156. Article 15(1) provides for limited exceptions to the right to the confidentiality of communications as provided for in Article 5 and other Articles of that Directive. Article 15(1) allows for restrictions on the scope of privacy rights "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, as referred to in Article 13(1) of Directive [95/46]." (See paragraph 11 of Judgment).

157. The national enactments at issue in *Tele2* were measures for the retention of communications data which were adopted as exceptions permitted by Article 15(1). As regards this kind of legislation, the ECJ concluded (at paragraph 78 of the Judgment) that a:

> *"… legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that Directive."*

158. In short, the Court's first conclusion was that national legislation establishing a system of general retention of communications data with a right of accessfor national authorities falls squarely within the scope of Directive 2002/58; and this conclusion in turn provided the legal basis for the subsequent holding that the validity of national legislation enacted pursuant to Directive 2002/58 fell to be determined by national courts by reference to EU law.

159. Having determined that national legislation of the kind in issue falls within the scope of EU law, the Court moved on to consider the first question posed in case C-203/15 (by the Swedish Court of Appeal), namely whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and 52(1) of the Charter:

"must be interpreted as precluding national legislation such as that in issue … [which] provides, for the purpose of fighting crime, for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications."

160. In this regard, the Court noted (at paragraph 63 of the Judgment) that:

"[t]hat question arises, in particular, from the fact that Directive 2006/24, which the national legislation at issue in the main proceedings was intended to transpose, was declared to be invalid by the Digital Rights judgment, though the parties disagree on the scope of that judgment and its effect on that legislation, given that it governs the retention of traffic and location data and access to that data by national authorities."

161. In the opinion of the Court, the principle of confidentiality of communications was established by Directive 2002/58. As stated in Article 5(1) of Directive 2002/58, that principle implies that, as a general rule, a person or entity is prohibited from storing communications data without the consent of the person to whom the data belongs. In addition, Service Providers are permitted to store transactional data only to the extent necessary for billing and marketing purposes; and thereafter are under a legal obligation to make the data anonymous.[27]

162. The only substantive exception to the principle of confidentiality of communications is that set out in Article 15(1) of the Directive permitting compulsory retention and disclosure of communications data in accordance with the provisions of that Article. The list of objectives for which a state may legislate for exceptions to the principles of confidentiality are precisely specified in Article 15(1), as supplemented by Article 13(1)

[27] See Article 6 of Directive 2002/58 and paragraph 86 of the Judgment in *Tele2*.

of Directive 94/46 to which Article 15(1) of Directive 2002/58 refers. Moreover, the list of recognised objectives is exhaustive and includes (as stated at paragraph 90 of the Judgment) safeguarding:

> *"national security – that is, state security – defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system."*

163. Bearing in mind that Article 15(1) must be interpreted in the light of the provisions of the EU Charter of Fundamental Rights, especially Articles 7, 8, 11 and 52(1) thereof, the Court then turned to consider the impact that the kind of data retention legislation under consideration may have on the fundamental rights of persons using electronic communications devices.

Rights Affected

164. As previously indicated, the Court identified (at paragraphs 100-101 of the Judgment) the Charter rights affected by a system of general and indiscriminate data retention established in domestic legislation as follows:

- The right to respect for private life and communications (Article 7).
- The right to the protection of personal data (Article 8).
- The right to freedom of expression (Article 11).

165. The wide extent of the impact of the impugned legislation on the aforementioned rights was a central concern for the Court, as can be seen clearly in the following quotation (from paragraph 98 of the Judgment):

> *"The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and*

type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, the Digital Rights judgment, paragraph 26)."

166. Then, in the ensuing paragraph, the Court turned to the impact of indiscriminate data retention legislation on the private lives of citizens:

"That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."

167. While underlining the importance of both the right to privacy and the right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter of

Fundamental Rights, the Court also laid emphasis on the right to freedom of expression as guaranteed by Article 11 of the Charter, stating, at paragraph 93 of the Judgment, that

> *"[t]hat fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society and is one of the values on which, under Article 2 TEU, the Union is founded … ".*

168. Accordingly, the Court observed (at paragraph 101 of the Judgment) that, even if data retention legislation does not permit the retention of the content of communications data

> *"it could nonetheless have an effect on the use of means of electronic communication, and consequently on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter."*

169. Given the seriousness of the interference with fundamental rights occasioned by the operation of a compulsory and indiscriminate data retention system, the Court concluded that insofar as data retention was permissible for the recognised purpose of combating crime, "*only the objective of fighting serious crime is capable of justifying such a measure …*".[28]

170. The Court then went on to add, at paragraph 103 of the Judgment:

> *"Further, while the effectiveness of fighting against serious crime, in organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot itself justify that national legislation providing for the general indiscriminate retention of all traffic*

[28] *Tele2* paragraph 102.

and location data should be considered necessary for the purposes of that fight …".

171. Here the Court was concerned that the effect of the impugned legislation was to make indiscriminate data retention the rule without exception, ''*whereas the system put in place by Directive2002/58 requires the retention of data to be the exception*.''

172. All of the foregoing considerations (along with others to be rehearsed later) led the Court to its first important and definitive conclusion about the impugned legislation, namely, that it cannot be considered to be justified in a democratic society. The Court stated, at paragraph 107 of the Judgment:

"National legislation such as that in issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter."

173. It might be convenient to note at this point that while the ECJ expressed definitive views on the incompatibility of the impugned national legislation with EU law, in the final analysis it is for the courts of individual Member States to decide whether their own national legislation should be struck down or disapplied in accordance with EU law as laid down by the ECJ. National courts are, of course, obliged to apply the principles set out by the ECJ; and any individual who considers that national law breaches their EU law rights has a variety of remedies under EU law.

174. Moreover, as previously indicated, the holding in *Tele2* does not preclude Member States from adopting a system of data retention and disclosure at national level. On the contrary, at paragraphs 108 to 111 of the Judgment the Court set out a number of principles and criteria with which national legislation must conform in order to comply with the requirements of EU law and, in particular, Article 15(1) of Directive 2002/58. These matters will be referred to later.

175. First, a brief look at the Court's response to the issues raised by the second question posed by the Swedish national court, namely, to ascertain:

> *" whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection of security of traffic and location data, and more particularly, the access of the competent national authorities to retained data, where the legislation does not restrict that access solely to the objective of fighting serious crime, where that access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned be retained within the European Union."*

176. It should be noted at the outset that the Court's unequivocal answer to that question was that EU law does indeed preclude such legislation.

177. In the opinion of the Court, access to retained communications data in the context of fighting crime must be restricted solely to fighting *serious* crime. Moreover, access by national authorities to such data must be the subject to prior review by a court or independent authority. In addition, Member States are obliged to ensure that retained data is stored within the European Union and thus within the purview of protection afforded by EU law.

178. In reaching its conclusions, the ECJ identified a range of fatal flaws or frailties in the kind of legislation at issue in the proceedings. In the result, the Court also identified, albeit in broad terms, the standards to which legislation establishing a system of retained communications data must conform in order to comply with EU law. In particular, the Court drew attention to the principle of proportionality as the primary mechanism for protecting the fundamental rights of citizens by limiting the scope of data retention and disclosure legislation to what is strictly necessary in the pursuit of legitimate objectives.

179. As we have seen, the Court underlined that the objectives which may be pursued by data retention and disclosure legislation are those referred to in Article 15(1) of Directive 2002/58. Such objectives constitute an exhaustive list of the purposes for which data retention and disclosure legislation may be enacted by way of exception to the general rule that communications data are strictly confidential.

Summary and Conclusions

180. The broad concordance between EU and ECHR law on the issue of data retention and disclosure has already been mentioned. It should be emphasised, however, that agreement between the two streams of law has by and large been centred on the application of the principle of proportionality when deciding the extent to which interference with fundamental rights in the matter of data retention is permissible for legitimate purposes. This in turn has led to a common approach on the kind of safeguards which should be included in data retention and disclosure legislation.

181. It will be recalled that the judgment of the ECJ in *Digital Rights Ireland* did not question the legitimacy of the general and indiscriminate retention of communications data as envisaged by Directive 2006/24. The essential reason why the ECJ found that Directive to be invalid was because it breached the principle of proportionality by failing to provide for sufficient safeguards to ensure that the otherwise legitimate interference with rights only went as far as was strictly necessary for the purpose for which the legislation was enacted. This is very much in line with the approach of the ECtHR to the issue of surveillance of communications and the right to privacy. Essentially this approach holds that it is permissible for a state to establish a system of general and indiscriminate data retention provided it is limited to what is strictly necessary in a democratic society for the achievement of a legitimate purpose, has a clear legal basis and is accompanied by safeguards that ensure compliance with the principle of proportionality.

182. However, the judgment of the ECJ in *Tele2*marked a departure from that approach in fundamental respects. The main finding of the Court in this regard was that legislation

of the kind in issue was in breach of "Article 15(1) of Directive 2002/58/EC...read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union". Article 5 of Directive 2002/58 makes statutory provision for the protection of the confidentiality of communications. Article 5 also expressly prohibits the storage or other kinds of surveillance of communications data, subject only to exceptions authorised by Article 15(1) which the Court stated must be strictly construed.

183. Thus the ECJ did not scrutinise the national legislation in issue on the basis of an autonomous or stand-alone application of the relevant Articles of the Charter. Rather it examined the regime established by national legislation from the perspective of its compatibility with an EU Directive, as interpreted in the light of Charter provisions. It may be said in conclusion that the rationale of the Court on this point is at times somewhat obscure. At the very least, it leaves room for speculation as to what the position would be under EU law if Directive 2002/58 was amended and express provision made for data retention regimes of the kind in issue as substantive measures rather than as exceptions to a general rule precluding such regimes under a strictly construed exception provision as laid down in Article 15(1). Whatever implications such a change in EU legislation might have for the scope of a data retention regime, it is unlikely that the need for safeguards would be any less.

184. Be that as it may, the central finding in *Tele2*is clear: legislation providing for a system of general and indiscriminate communications data retention without exception is precluded by Article 15(1) of Directive 2002/58/EC. By the same token, as the discussion and analysis in Chapter 1 illustrate, it is also clear that the blanket data retention measures imposed by the Communications (Retention of Data) Act, 2011 are in essence indistinguishable from those impugned in *Tele2*, and, consequently, that the 2011 Act will eventually have to be amended in order to conform with the requirements of EU law as articulated by the ECJ in that case – assuming, of course, that public policy remains committed to the idea of data retention and disclosure in its newly attenuated form.

185. Finally, it should be noted that the decision in *Tele2*has important implications even for a system of data retention and disclosure whose footprint has been shrunk in line with an outright ban on general and wholly indiscriminate retention. Even a system refashioned to take account of a blanket ban in this respect must be accompanied by a raft of safeguards, enjoying the force of law, designed to ensure that its retention and disclosure arrangements interfere with fundamental rights only to the extent that is strictly necessary for the achievement of legitimate purposes. As will be seen in Chapter 3, these safeguards go to the conditions of data retention and storage, criteria of access to data, and independent monitoring and regulation of the operation of the system of data retention and disclosure.

POSITION UNDER ECHR LAW

Introduction

186. The relevance of ECHR law as a reference point for national legislation on the retention of communications data has already been noticed. Suffice it to refer for present purposes to section 2 of the European Convention on Human Rights Act 2003 which requires a court "in interpreting and applying any statutory provision or rule of law … insofar as is possible, … [to] do so in a manner compatible with the State's obligations under the Convention provisions."Given the substantial correlation between ECHR law and EU law in the matter of data retention, the Review did not consider it necessary to prosecute a detailed analysis of the decisions of the ECtHR in this area. Accordingly, what follows is no more than a *tour d'horizon* of that court's most salient observations on the rights affected by data retention systems, and the safeguards needed to protect those rights from undue infringement.

187. For the purposes of this presentation, the key provisions of the ECHR are as follows:

Article 8:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right accept such as is in accordance with the law and is necessary in a democratic society … "

Article 10:

"1. Everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by a public authority and regardless of frontiers. …

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties are prescribed by law and are necessary in a democratic society, … "

Right to Privacy

188. The ECtHR has consistently recognised that both the interception and retention of personal data constitute an interference with the right to privacy:

"33. Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence…"

Kruslin v. France (24 April 1990)

"78. … the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily

strikes at freedom of communication between users of the communications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them*." (emphasis added)*

Weber and Saravia(admissibility decision)(29 June 2006)

"67. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence]... The subsequent use of the stored information has no bearing on that finding ... However, in determining whether the personal information retained by the authorities involves any ... private-life [aspect] ..., the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ..."

S. and Marper v. United Kingdom (4 December 2008) [GC]

"53…Given the technological advances since the Klass and Others case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely. (see Copland v. the United Kingdom, no. 62617/00, § 41, ECHR 2007-I).

…

"70. The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile … of the most intimate aspects

of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union *and the European Parliament (see paragraphs 23 and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices.*" (emphasis added)

Szabó and Vissy v. Hungary (12 January 2016)

189. Of particular relevance in the present context is *Malone v. United Kingdom* where the Court rejectedthe UK government's argument that "metering" (the use of a meter check printer, i.e. a Post Office device which registers the numbers dialed on a particular telephone and the time and duration of each call) did not raise any issue of interference under Article 8 ECHR:

"84. As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8. The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent

of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8."

190. In that case the Court found a violation of Article 8 even though the matter at issue was a much more limited form of data retention and disclosure than the regime under consideration in this Review.

191. On a more general level, the Court recently recognized the threat posed to Convention rights by new technologies of data collection in *Szabó and Vissy v.Hungary*:

"68. For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen … especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive

power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Unionand, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information (see paragraphs 23 and 24 above)."

Szabó and Vissy v. Hungary (12 January 2016)

Limits to Right to Privacy

192. The ECtHR has emphasised that interference with the right to private life under Article 8 ECHR must fall within the four corners of the exceptions set out in paragraph 2 of that Article, and has set down detailed guidance regarding the various requirements specified in that paragraph (i.e. that interference must be "in accordance with law and necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others").

193. In the cases dealing with Article 8.2, particular attention has been given to 'the interests of national security' and 'the prevention of disorder or crime' rubrics, given that these are also grounds of access to retained data under the 2011 Act. It may be noted in this regard that 'the saving of human life' rubric in section 6 the 2011 Act falls within the public safety exception in Article 8(2).

194. Reflecting its broad interpretation of the right to privacy in Article 8(1) ECHR, the Court has been at pains to stress that the exceptions to the right set out in Article 8(2) must be interpreted narrowly:

"54. Any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to

which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim. This provision, "since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions" (see Klass and Others, cited above, § 42).

Szabó and Vissy v. Hungary (12 January 2016)

195. That said, the Court has also recognized the real-world challenges faced by States in addressing crime and terrorism, and while it has been prepared to subject legislative measures dealing with such problems to searching scrutiny, it has accorded a significant margin of appreciation to these measures in several important cases. In *Klass v. Germany*, the Court set out an overarching framework of principle for dealing with these difficult problems:

> *"49. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field (cf., mutatis mutandis, the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, pp. 45-46, para. 93, and the Golder judgment of 21 February 1975, Series A no. 18, pp. 21-22, para. 45; cf., for Article 10 para. 2, the Engel and others judgment of 8 June 1976, Series A no. 22, pp. 41-42, para. 100, and the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, para. 48).*
>
> *Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance.* The Court, being aware of the

danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.

50. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. *This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."(emphasis added)*

Klass v. Germany (6 September 1978)

In Accordance with Law: Clarity, Accessibility and Foreseeability

196. It is noteworthy that the Court regards this rubric as going beyond mere conformity with positive domestic law; in addition to the principle of legality, it also comprehends the important codification principles of clarity, accessibility, and foreseeability in compliance with higher legal norms by which states are bound:

"95. The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the

competent authorities and the manner of its exercise (see Malone v. the United Kingdom, 2 August 1984, §§ 66-68, Series A no. 82; Rotaru v. Romania [GC], no. 28341/95, § 55, ECHR 2000-V; and Amann, cited above, § 56). (emphasis added)

96. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed (see Hasan and Chaush v. Bulgaria [GC], no. 30985/96, § 84, ECHR 2000-XI, with further references).”

S. and Marper v. United Kingdom (4 December 2008) [GC]

197. In this connection, the Court has stated that the rules governing interception of telephone communications must abide by the legality, foreseeability and clear statement principles:

“229. The Court has held on several occasions that the reference to “foreseeability” in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident*. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on [sic] which public authorities are empowered to resort to any such measures.” (emphasis added)*

…

236. …The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards andguarantees against abuse.

Roman Zakharov v. Russia (4 December 2015) [GC]

198. In *S. and Marper v. United Kingdom* the Court followed this reasoning in the context of *the storage of personal data*, emphasizing that a U.K. legal framework must be detailed and precise, and must contain minimum safeguards to protect against abuse:

"98. As regards the conditions attached to and arrangements for the storing and use of this personal information, section 64 is far less precise. It provides that retained samples and fingerprints must not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

99. The Court agrees with the applicants that at least the first of these purposes is worded in rather general terms and may give rise to extensive interpretation. It reiterates that it is as essential, in this context, as 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 of 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 (see, mutatis mutandis, Kruslin v. France, 24 April 1990, §§ 33 and 35, Series A no. 176‑A; Rotaru, cited above, §§ 57-59; Weber and Saravia v. Germany*

(dec.), no. 54934/00, ECHR 2006-XI; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, §§ 75-77, 28 June 2007; and Liberty and Others v. the United Kingdom, no. 58243/00, §§ 62-63, 1 July 2008). The Court notes, however, that these questions are in this case closely related to the broader issue of whether the interference was necessary in a democratic society. In view of its analysis in paragraphs 105-26 below, the Court does not find it necessary to decide whether the wording of section 64 meets the 'quality of law' requirements within the meaning of Article 8 § 2 of the Convention." (emphasis added)

S. and Marper v. United Kingdom (4 December 2008) [GC]

199. In the earlier case of *Malone v. United Kingdom*, referred to briefly above, the Court noted that the practice whereby the Post Office provided "metering" records to the police (containing information on numbers dialed on a particular telephone and the time and duration of each call) was legal under domestic law, but did not satisfy the Convention requirement of being "in accordance with the law" because it failed to address "*the scope and manner of exercise of the discretion enjoyed by public authorities*": (emphasis added)

"86. In England and Wales, although the police do not have any power, in the absence of a subpoena, to compel the production of records of metering, a practice exists whereby the Post Office do on occasions make and provide such records at the request of the police if the information is essential to police enquiries in relation to serious crime and cannot be obtained from other sources (see paragraph 56 above). The applicant, as a suspected receiver of stolen goods, was, it may be presumed, a member of a class of persons potentially liable to be directly affected by this practice. The applicant can therefore claim, for the purposes of Article 25 (art. 25) of the Convention, to be a "victim" of a violation of Article 8 (art. 8) by reason of the very existence of this practice, quite apart from any concrete measure of implementation taken against him (cf., mutatis mutandis,

paragraph 64 above). This remains so despite the clarification by the Government that in fact the police had neither caused his telephone to be metered nor undertaken any search operations on the basis of any list of telephone numbers obtained from metering (see paragraph 17 above; see also, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p. 20, para. 37 in fine).

"87. Section 80 of the Post Office Act 1969 has never been applied so as to 'require' the Post Office, pursuant to a warrant of the Secretary of State, to make available to the police in connection with the investigation of crime information obtained from metering. On the other hand, no rule of domestic law makes it unlawful for the Post Office voluntarily to comply with a request from the police to make and supply records of metering (see paragraph 56 above). The practice described above, including the limitative conditions as to when the information may be provided, has been made public in answer to parliamentary questions (ibid.). However, on the evidence adduced before the Court, apart from the simple absence of prohibition, there would appear to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities. Consequently, although lawful in terms of domestic law, the interference resulting from the existence of the practice in question was not 'in accordance with the law', within the meaning of paragraph 2 of Article 8 (art. 8-2) (see paragraphs 66 *to 68 above). (emphasis added)*

"88. This conclusion removes the need for the Court to determinewhether the interference found was 'necessary in a democratic society' for one of the aims enumerated in paragraph 2 of Article 8 (art. 8-2) (see, mutatis mutandis, paragraph 82 above)."

Malone v. United Kingdom (2 August 1984)

200. It is important to notice that the Court has recognised that respect for the legality, clear statement, and foreseeability principles does not entail unrealistic levels of precision in the applicable rules. In the context of Hungarian State laws permitting surveillance for "the prevention, tracking and repelling of terrorist acts in Hungary" and "the gathering of intelligence necessary for rescuing Hungarian citizens in distress abroad", the Court rejected the applicants' arguments that these terms were too vague, although it stressed that a law cannot confer unfettered power on security agencies:

> *"64. The Court is not wholly persuaded by this argument, recalling that the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague (see Kokkinakis v. Greece, 25 May 1993, § 40, Series A no. 260-A). It is satisfied that even in the field of secret surveillance, where foreseeability is of particular concern, the danger of terrorist acts and the needs of rescue operations are both notions sufficiently clear so as to meet the requirements of lawfulness. For the Court, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication (compare and contrast Iordachi and Others, cited above, § 46). For the Court, nothing indicates in the text of the relevant legislation that the notion of "terrorist acts", as used in section 7/E (1) a) (ad) of the Police Act, does not correspond to the crime of the same denomination contained in the Criminal Code (see paragraph 16 above).*
>
> *65. However, in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the*

sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference *(see Roman Zakharov, cited above, § 247*)." (emphasis added)

Szabó and Vissy v. Hungary (12 January 2016)

Necessary in a Democratic Society

201. The foregoing survey illustrates that where an impugned legislative measure comes within the exceptions under Article 8(2) ECHR (here, national security or the prevention of crime), the Court's assessment of whether the measure is necessary in a democratic society hinges firstly on its proportionality and secondly on whether it provides sufficient safeguards against abuse and arbitrariness.

202. In *Malone v. United Kingdom* (the "metering" case discussed above), the Court emphasised that the potentially harmful consequences of the so called "metering" practice (whereby intercepted data was handed over to the police) could only be considered to be necessary in a democratic society if it contained sufficient protections against abuse:

"81. Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2) (see, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p. 23, para. 48). The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals

and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime". However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (ibid., p. 26, para. 56). This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse (ibid., p. 23, paras. 49-50)." (emphasis added

Malone v. United Kingdom (2 August 1984)

203. In S. and Marper v. United Kingdom the Court set out the general principles governing data retention:

"101. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the *Court for conformity with the requirements of the Convention (see Coster v. the United Kingdom [GC], no. 24876/94, § 104, 18 January 2001, with further references).*

102. A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will

tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see Connors v. the United Kingdom, no. 66746/01, § 82, 27 May 2004, with further references). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see Evans v. the United Kingdom [GC], no. 6339/05, § 77, ECHR 2007-I). Where, however, there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider (see Dickson v. the United Kingdom [GC], no. 44362/04, § 78, ECHR 2007-V).

103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article(see, mutatis mutandis, Z v. Finland, cited above, § 95). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention and the Preamble thereto and Principle 7 of Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector).The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention). The above considerations are especially valid as regards the protection of special categories of more sensitive data (see

Article 6 of the Data Protection Convention) and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family (see Recommendation No. R (92) 1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system).(emphasis added)

104. The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (see Article 9 of the Data Protection Convention). However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned (see, mutatis mutandis, Z v. Finland, cited above, § 96)."

S. and Marper v. United Kingdom (4 December 2008) [GC]

204. Albeit in the context of a law permitting blanket secret surveillance with few safeguards, the following statement of the Court in *Szabó v. Hungary* is also apposite in this regard:

"73. …given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement 'necessary in a democratic society' must be interpreted in this context as requiring 'strict necessity' in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions [sic] and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to

these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to *answer to strict necessity (see paragraphs 23 and 24 above) – an approach it considers convenient to endorse. Moreover, particularly in this context the Court notes the absence of prior judicial authorisation for interceptions, the importance of which will be examined below in paragraphs 75 et seq. This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of 'persons concerned identified ... as a range of persons' by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case (see, mutatis mutandis, Roman Zakharov, cited above, § 249). It is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied (see Roman Zakharov, cited above, § 266)."*

Szabó and Vissy v. Hungary (12 January 2016)

Proportionality Principle

205. In line with the general thrust of the Court's jurisprudence, the question of whether a given legislative measure is "necessary in a democracy" is ultimately determined by reference to the proportionality principle. Although the Court's implementation of the proportionality test can be somewhat unclear from case to case, it may be said that a measure interfering with personal data, and therefore amounting to an interference with the right to privacy in Article 8 ECHR, is more likely to pass the proportionality test the more it contains strong safeguards or protections for affected rights.

206. When assessing a data retention system in light of the principle of proportionality, the Court tends to look at the totality of the statutory system governing interference with personal data, with the result that there is no hard and fast rule concerning the form of the system. However, the Court's jurisprudence tends to focus on several key safeguards as indicia of proportionality. In the context of data retention systems, these include ex ante controls; post factum controls; requirements for subsequent notification; restrictions on the length of time data is retained; restrictions on the use of data; and rules on the destruction of data.

Ex Ante and Post Factum Controls

207. The Court's jurisprudence does not disclose a general requirement of prior independent control of applications for access to retained data. The ECtHR has found that in certain circumstances subsequent, or post factum, control of access to private data by an independent administrative or judicial authority may constitute a sufficient safeguard in lieu of prior control. It will be recalled that EU law now requires prior independent judicial or administrative control of access by state authorities to retained communications data.

Subsequent Notification

208. In *Szabó* the Court indicated that subsequent notification is required as soon as it can be effected without endangering the purpose of a surveillance measure (this principle was developed from *Klass* onwards, and clearly stated in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* in 2007, although these cases are not cited in the following passage):

> *"86. Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the*

latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned (see Weber and Saravia, cited above, §135; Roman Zakharov, cited above, § 287). In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates that the legislation falls short of securing adequate safeguards.

87. It should be added that although the Constitutional Court held that various provisions in the domestic law read in conjunction secured sufficient safeguards for data storage, processing and deletion, special reference was made to the importance of individual complaints made in this context (see point 138 of the decision, quoted in paragraph 20 above). For the Court, the latter procedure is hardly conceivable, since once more it transpires from the legislation that the persons concerned will not be notified of the application of secret surveillance to them.

88. Lastly, the Court notes that is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples (see Roman Zakharov, cited above, § 284). However, the Government were not able to do so in the instant case."

Szabó and Vissy v. Hungary (12 January 2016)

209. Although taken from a case dealing with targeted surveillance as opposed to data retention, if the following paragraph can be taken as containing statements of general principle, it will be seen that the 2011 Act falls short of ECHR standards on several fronts including lack of ex ante control outside the executive, uncertainty as to the precise standard applied in practice for permitting access, and the adequacy and effectiveness of the safeguards and remedies available:

"89. In total sum, the Court is not convinced that the Hungarian legislation on "section 7/E (3) surveillance" provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures.

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."

Szabó and Vissy v. Hungary(12 January 2016)

Data Retention, Use and Destruction Rules

210. As already indicated, the Court has expressed strong reservations about the indefinite retention of personal data. Second, the Court has frequently emphasised the importance of clear rules on the use and destruction of retained data. Third, as is clear from the judgment excerpted below, the Court considers independent review as crucial in assessing the rules on data retention.

211. The leading judgment here is *S. and Marper v. United Kingdom*, which concerned a challenge to the indefinite retention in a database of the applicants' fingerprints, cell samples and DNA profiles after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in another. The Court held that there had been a violation of Article 8 ECHR, on the basis that the retention at issue constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society. The Court considered in particular that the use of modern scientific techniques in the criminal justice system could not be allowed at any cost and without carefully balancing the potential benefits of the extensive

use of such techniques against important private life interests. The Court held that any State claiming a pioneer role in the development of new technologies (as the UK did here) bears special responsibility for "striking the right balance". The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests.

> *"111. The Government lay emphasis on the fact that the United Kingdom is in the vanguard of the development of the use of DNA samples in the detection of crime and that other States have not yet achieved the same maturity in terms of the size and resources of DNA databases. It is argued that the comparative analysis of the law and practice in other States with less advanced systems is accordingly of limited importance.*
>
> *112. The Court cannot, however, disregard the fact that, notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life. The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully* balancing the potential benefits of the extensive use of such techniques against important private-life interests*. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.*

…

117. While neither the statistics nor the examples provided by the Government in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position, the Court accepts that the extension of the database has nonetheless contributed to the detection and prevention of crime.

118. The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests.

119. In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the national database or the materials destroyed (see paragraph 35 above); in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

120. The Court acknowledges that the level of interference with the applicants' right to private life may be different for each of the three different categories of personal data retained. The retention of cellular samples is particularly intrusive given the wealth of genetic and health information contained therein. However, such an indiscriminate and open-ended retention regime as the one in issue calls for careful scrutiny regardless of these differences.

121. The Government contend that the retention could not be considered as having any direct or significant effect on the applicants unless matches in the database were to implicate them in the commission of offences on a future occasion. The Court is unable to accept this argument and reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data *(see paragraph 67 above).*

…

125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to

the personal data concerned and insufficient protection against the misuse or abuse of such data.

126. Accordingly, there has been a violation of Article 8 of the Convention in the present case."

S. and Marper v. United Kingdom (4 December 2008) [GC]

General Conclusions on ECHR

212. As is clear from the foregoing overview of its case law, the ECtHR has been consistently critical of all forms of state surveillance of electronic communications, including the retention of communications data. In the opinion of the Court, surveillance of private data by the state poses a serious threat to fundamental rights - of citizens and journalists alike -and is especially prone to abuse when state authorities, and in particular police authorities, are given secret or discretionary access to such data.

213. Accordingly, in line with the corresponding case law of the ECJ, national statutory measures for the retention of communications data can only be justified under the Convention if they are proportionate and necessary in a democratic society and subject to extensive safeguards designed to ensure that they do not exceed these limits. Thus it follows that national legislation providing for data retention and disclosure should reflect the disaggregation of these basic concepts as elaborated in the case law of the ECtHR in respect of the fundamental rights of citizens generally, and, in the case of journalists, in the matter of the confidentiality of journalistic sources. (**R**)

SPECIAL PROTECTION OF JOURNALISTS' SOURCES

214. The foregoing discussion of the protection of fundamental rights and in particular the right to privacy under the ECHR was within the context of the protection of the rights to privacy of all persons, including journalists. As already explained, this is because the law and principles governing the protection of a journalist's right to privacy in relation to his or her retained communications data are those which apply to persons or citizens generally,

without any distinction as to occupation. Accordingly, it was necessary to examine the law and principles protecting the fundamental rights of persons generally in order to identify those upon which journalists are entitled to rely.

215. On the other hand, issues concerning the "principle of protection of journalistic sources" referred to in the Terms of Reference is unique to journalists, and is of vital importance to them in the exercise of their professional activities.

216. There are three sources of law and obligations that must be taken into account when seeking to define or enact legislative policy on the protection of journalistic sources. These are the Constitution, the ECHR and EU law. Insofar as the Irish courts, in particular the Supreme Court, have pronounced on this issue, the principles relied upon essentially mirror those set out in the case law of the ECtHR. As will be seen presently, the ECJ has not had occasion to pronounce directly on the issue of the protection of journalistic sources. However, the limitations and extensive safeguards laid down by that court in *Tele2* as essential accompaniments of a communications data retention regime have obvious implications for the protection of journalistic sources where access to communications data has been sought for purposes which may include ascertaining such sources.

217. In contrast, the ECtHR has had the opportunity to examine in detail the issues surrounding the principle of protection of journalistic sources, including the strictly limited circumstances in which there may be exceptions to that principle. Accordingly, it is proposed to consider its approach first.

ECHR Principles

218. The ECtHR largely anchors the protections which must be afforded to journalists seeking to maintain the confidentiality of their sources in Article 10 guaranteeing freedom of expression including a free media which the Court sees as a structural support for democratic governance. Thus the Court has held that any limitation on the principle of freedom of expression may have a detrimental impact not only on journalists and their

sources, but also on the publication concerned and, indeed, the public generally, the latter having an interest in receiving information furnished by such sources.

> *"39. The Court recalls that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance (see, as a recent authority, the Jersild v. Denmark judgment of 23 September 1994, Series A no. 298, p. 23, para. 31). 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 information be adversely affected. … [A]n order of source disclosure ...cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest."*
>
> *Goodwin v. the United Kingdom* (27 March 1996) [GC]

219. In the opinion of the Court, the principle of confidentiality of journalistic sources is based on the right to freedom of expression guaranteed by Article 10 ECHR, rather than the right to private and family life in Article 8, notwithstanding that these two rights may on occasion intersect in practice. Moreover, as Article 10(2) illustrates, the principle of confidentiality of journalistic sources is not absolute:

> *"The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity of public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or maintaining authority and impartiality of the judiciary."*

220. However, exceptions to the principle of confidentiality of journalistic sources must be justified by an "overriding requirement in the public interest". Interestingly, this approach is mirrored in Irish law: *Mahon & Others v. Keena* [2010] 1Rand *Cornec v. Morrice* [2012] 1 IR 804. In the first of these cases the Supreme Court found that exceptions to the principle of confidentiality of journalistic sources could only be "justified by an overriding requirement in the public interest" (at paragraph 69 of the Judgment of Fennelly J.) The Court also noted that the relevant legislation and any rule of law should, in accordance with the provisions of section 2 of the European Convention on Human Rights Act, 2003 be interpreted in "a manner compatible with the State's obligations under the Convention provisions.''

221. The ECtHR provided a valuable overview of its approach to freedom of expression and the exceptions thereto in *Financial Times v. United Kingdom.* It will be seen that the Court refers expressly to the requirement of a "pressing social need" for interference with the right to freedom of expression, but does not always use this phrase in the context of the right to privacy cases discussed earlier (*S. and Marper v. United Kingdom* is a notable exception in this regard). All of which suggests more intense judicial scrutiny where media and free speech concerns are to the fore:

> *"60. The Court recalls that as a matter of general principle, the "necessity" of any restriction on freedom of expression must be convincingly established. It is for the national authorities to assess in the first place whether there is a "pressing social need" for the restriction and, in making their assessment, they enjoy a certain margin of appreciation. In the present context, however, the national margin of appreciation is circumscribed by the interest of democratic society in ensuring and maintaining a free press. This interest will weigh heavily in the balance in determining whether the restriction was proportionate to the legitimate aim pursued.* The Court reiterates that limitations on the confidentiality of

journalistic sources call for the most careful scrutiny by the Court (Goodwin, cited above, §40).

61. The Court's task, in exercising its supervisory function, is not to take the place of the national authorities but rather to review the case as a whole, in the light of Article 10, and consider whether the decision taken by the national authorities fell within their margin of appreciation. The Court must therefore look at the interference and determine whether the reasons adduced by the national authorities to justify it are "relevant and sufficient" (Handyside v. the United Kingdom, 7 December 1976, § 50, Series A no. 24 and Goodwin, cited above, § 40).

62. The Court reiterates that under the terms of Article 10 § 2, the exercise of freedom of expression carries with it duties and responsibilities which also apply to the press. Article 10 protects a journalist's right – and duty – to impart information on matters of public interest provided that he is acting in good faith in order to provide accurate and reliable information in accordance with the ethics of journalism (Fressoz and Roire v. France [GC], no. 29183/95, § 54, ECHR 1999-I and Bladet Tromsø and Stensaas v. Norway[GC], no. 21980/93, § 65, ECHR 1999-III).

63. In the case of disclosure orders, the Court notes that they have a detrimental impact not only on the source in question, whose identity may be revealed, but also on the newspaper against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on the members of the public, who have an interest in receiving information imparted through anonymous sources and who are also potential sources themselves (see, mutatis mutandis, Voskuil v. the Netherlands, no. 64752/01, § 71, 22 November 2007). While it may be true that the public perception of the principle of non-disclosure of sources would suffer no real damage where it was overridden in

circumstances where a source was clearly acting in bad faith with a harmful purpose and disclosed intentionally falsified information, courts should be slow to assume, in the absence of compelling evidence, that these factors are present in any particular case. In any event, given the multiple interests in play, the Court emphasises that the conduct of the source can never be decisive in determining whether a disclosure order ought to be made but will merely operate as one, albeit important, factor to be *taken into consideration in carrying out the balancing exercise required under Article 10 § 2." (emphasis added)*

Financial Times and Others v. United Kingdom (15 December 2009)

222. The Court has recognised that the need for ex ante or prior judicial control is greater in respect of secret surveillance of the media by the state, especially when the confidentiality of sources cannot be restored by remedial measures:

"77. …The Court recalls that the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see Klass and Others, cited above, §§ 55 and 56). The Court recalls that in Dumitru Popescu (cited above, §§ 70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see Klass and Others, cited above, §§

42 and 55). The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation (see Kennedy, cited above, § 167). Indeed, in certain respects and for certain circumstances, the Court has found already that ex ante (quasi-judicial) authorisation is necessary, for example in regard to secret surveillance measures targeting the media. In that connection the Court held that a post factum review cannot restore the confidentiality of journalistic sources once it is destroyed (seeTelegraaf Media Nederland *Landelijke Media B.V. and Others v. the Netherlands, no. 39315/06, § 101, 22 November 2012; for other circumstances necessitating ex anteauthorisation see Kopp v. Switzerland, 25 March 1998, Reports 1998 II).* (emphasis added)

Szabó and Vissy v. Hungary (12 January 2016)

223. In the result, it may be said that the ECtHR's approach to the issue of exceptions to the confidentiality of journalistic sources is based on the following principles:

- The exception must be justified by an overriding requirement in the public interest.
- The necessity for the exception must be assessed in light of an established "pressing social need"; and must be convincingly established on that basis.
- The onus rests on state authorities to adduce reasons which are "relevant and sufficient" to justify the necessity in the public interest for disclosure of journalistic sources.
- Any exception which permits the identification of journalistic sources or which might oblige a journalist to disclose them should be subject to prior control by a judicial or independent administrative authority.

224. Moreover, in deciding whether to permit or provide for an exception to the confidentiality of journalistic sources regard may be had to whether the journalist was acting in good faith - in order to provide accurate and reliable information in line with journalistic ethics - and in accordance with law. In addition, where a journalistic source wasclearly acting in bad faith - with a harmful purpose or by intentionally disclosing falsified information – this is a matter which may be taken into account in determining whether an exception to the principle of confidentiality is permissible. The conduct of the source may not be decisive in determining whether a disclosure of journalistic sources should be permitted but it is an important factor to be taken into consideration when carrying out a balancing exercise in this regard.

EU Law

225. In addition to the foregoing, Article 11 of the EU Charter contains the guarantee that "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." Paragraph 2 of Article 11 states: "The freedom and pluralism of the media shall be respected." There is a close correspondence between this guarantee in the EU Charter and the guarantee contained in the ECHR concerning freedom of expression. Article 52, paragraph 3 of the EU Charter provides that "Insofar as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection." The Review considers it safe to assume that the standards of protection for the confidentiality of journalistic sources would be no less under EU law than those applying under Convention law, particularly in regard to the rule that any exception to the confidentiality principle must be justified by an "overriding requirement in the public interest" (a principle also applicable under Irish Constitutional law).

226. As already stated, in light of the conclusions in the *Tele2* case, EU law now requires the application of a whole range of safeguards governing access by State authorities to any system for the general retention of communications data. While these safeguards are designed to protect the fundamental rights of all citizens including journalists, some of them might be considered of particular significance for the protection of journalistic source. These include:

227. The general principle stated in paragraph 119 of *Tele2* that, in relation to the objective of fighting serious crime, only the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime, may be accessed by State authorities. Thus, contrary to the position that appears to be permitted under the 2011 Act, a journalist's retained data should not be accessed for the purpose of investigating a crime allegedly committed by another person. (The ECJ acknowledges that there may be an exception to that general rule "in particular situations, "where, for example, vital national security interests of the State are threatened and other objective criteria for access are met.*"*);

228. Other than in exceptional cases of urgency, access to retained data should be subject to prior authorisation by a judge or independent administrative authority. Given the unique characteristics of any legitimate form of general retention of communications data (where such historical data is retained without consent, and even in respect of persons who are not or ever likely to be suspected of wrongdoing), and bearing in mind the special scrutiny which should apply to State surveillance of journalistic communications, it will be recommended that authorisations for access to journalists' retained data for the specific purpose of identifying their journalistic sources should be obtainable only from a judge of the High Court;

229. A journalist whose retained communications data has been accessed should subsequently be notified that such access has been obtained (for whatever purpose) as soon as such notification would no longer prejudice an investigation or prosecution of a serious criminal offence;

230. A journalist who considers that his or her legal rights have been infringed by reason of wrongful access by a statutory body to his or her retained communications data will have such remedies available to vindicate their rights as are recommended elsewhere in this Review in accordance with EU law requirements in respect of all persons who find themselves in this position.

Summary of Recommendations on Journalistic Sources

231. Applications by a statutory body for authorization to access a journalist's retained communications data for the specific purpose of determining his journalistic sources should be made only to a judge of the High Court. (**R**)

232. Access to a journalist's retained communications data for any purpose, including for the purpose of identifying his or her sources, should in principle be permitted only when the journalist is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State. **(R)**

233. Accordingly, contrary to what is permitted under the 2011 Act it should not be permissible to access a journalist's retained data for the purpose of investigating an offence committed by someone else. This limitation should be subject only to 'particular situations' (referred to at paragraph 119 of the *Tele2* Judgment) where vital national interests such as public security are at stake and there is objective evidence justifying access. **(R)**

234. In addition, as regards any statutory regime for the retention of communications data, express provision should be made by law prohibiting access by State authorities to retained data for the purpose of discovering a journalist's sources unless such access is fully justified by an overriding requirement in the public interest. (**R**)

235. A journalist whose retained communications data has been accessed should, as in the case of any other person similarly affected, be notified of that fact as soon as such

notification would no longer be likely to prejudice any investigation or prosecution of a serious criminal offence. (**R**)

236. The general recommendation that express provision be made for judicial remedies in the case of unlawful access of a person's retained communications data should, *ipso facto*, be available to journalists who considers their rights have been infringed by any such access. (**R**)

237. As already pointed out, in addition to these particular safeguards, access to a journalist's retained communications data for any purpose will also benefit from the full range of safeguards recommended in respect of such access generally by State authorities. (**R**)

CONFORMING LEGISLATION

Setting Outer Limits

238. The essential safeguard provisions of any amending legislation designed to conform to the combined requirements of EU and ECHR law in the matter of data retention and disclosure are discussed in detail in Chapter 3. However, before concluding this assessment of the role of fundamental rights in shaping any future legislation in this regard, it is necessary to refer to the permissible scope of any conforming data retention regime as conceived by the ECJ. First, bearing in mind the ECJ's radical conclusion in *Tele2* that a system of general and wholly indiscriminate data retention is incompatible with Article 15(1) of Directive 2002/58 on Privacy and Communications, as interpreted in light of the EU Charter of Fundamental Rights:

> *"… national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards so that persons whose data has been retained have sufficient guarantee of the effective protection of their personal data against the risk of misuse. That legislation must, in*

particular, indicate what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary …"(para. 109)

Second:

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

The Court then held (at paragraph 111 of the Judgment):

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

that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."

239. The difficulties surround the limitations laid down in *Tele2* on the permissible scope of a replacement data retention and disclosure regime will not be easily resolved by national legislatures. At paragraph 108 of its Judgment the ECJ characterized data retention legislation drafted to take account of the aforementioned limitations as "the targeted retention of traffic and location data". To say the least, it will not be easy to reconcile this notion of "targeted" retention with the idea of surveillance by means of some form of general data retention, on the one hand, and the long-standing practice of so-called ''targeted'' surveillance when used by police authorities as an investigatory tool, on the other. The latter is authorised and used under the aegis of legislation falling outside the remit of this Review. As explained in Chapter 1, "targeted" surveillance in this sense is focused on persons who have already been identified as being potentially connected, even indirectly, with serious crime. Targeted surveillance of this kind enables the competent authorities to access data relating to communications effected by individuals thus identified, even to the extent of accessing the content of their communications. However, the key point is that access is limited to communications made *after* one or more individuals have been identified as having a potential connection with serious crime.

240. In contrast, general data retention obligations relate to all communications effected by all users without requiring any connection whatsoever with serious crime. Moreover, these obligations enable competent authorities to access the communications history of persons who have not yet been identified as potentially connected with serious crime or terrorism. In this sense general data retention obligations give law enforcement authorities access to the past, allowing them to access communications made by users *before* any potential link with serious crime has been established.

241. This concern is reflected in the distinction made by the Advocate General in his Opinion in the *Tele2* case, at paragraphs 179 and 180. He went on to add, at paragraph 181:

"In other words, the usefulness of general data retention obligations in the fight against serious crime lies in its limited ability to examine the past by consulting the data that retraces the history of communications effected by persons even before they are suspected of being connected with a serious crime."

242. As already indicated, the ruling in *Tele2* precludes a system of wholly indiscriminate communications data retention applying to the public at large on the grounds that it is incompatible with EU law, including Article 15(1) of Directive 2002/58. Moreover, we have seen that the ruling nevertheless allows for a form of communications data retention where, on the basis of objective evidence, it is possible to identify "*a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, …",* and thus to contribute to fighting serious crime or preventing a serious risk to public security. In the opinion of the Court, in a scheme of this kind the relevant public might be confined by geographical area or population segment.

243. In the opinion of the Review, selecting an identifiable and limited segment of the public (for example, in a town, suburb, or region) on the basis of objective links with serious crime or terrorism is likely to give rise to serious difficulties for investigatory bodies, not to mention concerns that a system designed on these lines will discriminate against particular sections of the public or particular regions or cities. Moreover, it must be borne in mind that even a form of data retention limited by geography or population subset will necessarily involve retaining the data of wholly innocent persons, of all ages, who are not suspected or ever likely to be suspected of wrongdoing. In this sense, the replacement data retention system contemplated by the ECJ in *Tele2 s*uffers from the principal frailty associated with a scheme of universal retention: it will still be indiscriminate in application, albeit on a more limited scale.

244. The reasoning in *Tele2* also seems to rest on the assumption – never made explicit – that, once identified, persons suspected of involvement in serious criminal activity or terrorism are likely to 'turn up' in one section of the public or geographical area rather

than another. While this may be true in some cases, it will be of no assistance where a suspect is operating outside the 'targeted' public or geographical area. In these circumstances it will not be possible to trace a suspect's communications history by accessing his retained data in accordance with established safeguards since, by definition, no such data will exist in respect of that person. Unfortunately, these difficulties were not given an airing in *Tele2*.

245. The aforementioned limitations on the permissible scope of any data retention system may well deprive national authorities of important strategic options in investigating terrorist and other serious crime. The difficulties which legislators are likely to encounter in seeking to fashion an effective system of communications data retention within the limited or 'targeted' confines laid down by the ECJ in *Tele2* may cause Member States to consider, from a policy perspective, whether EU law in this area, including Article 15(1) of Directive 2002/58, should be amended.

246. These difficulties notwithstanding, the ECJ's dicta, cited above, on the permissible scope of any compulsory data retention regime provide the framework of EU law principles with which any new legislation on the subject must comply in order to constitute a lawful exception within the meaning of Article 15(1) of Directive 2002/58.

247. Finally, if legislation is adopted within that framework, it seems the resultant national data retention scheme may have to include provision for the possible extension, from time to time, of its application to a region or a section of the public whose data should be retained under the umbrella of the parent Act according as objective evidence arose for the need for such a course of action. To say the least, it would be unreal to expect such extending measures to be done by way of amending legislation given the length of time such a process inevitably takes. Accordingly, legislation establishing a data retention system as envisaged by the ECJ in *Tele2* should include within its provisions the power to extend the application of a data retention regime from time to time in accordance with the criteria referred to by the ECJ. One means of doing this would be by Ministerial Order or Regulation. Any power to extend the application of an existing data

retention regime along these lines would have to be framed by reference to clearly defined objective criteria for the exercise of such a power. (**R**)

Reach of Proportionality Principle

248. The way forward is a lot clearer in respect of the safeguards which both the ECJ and, in broad measure, the ECtHR believe conforming legislation must include in order to ensure that the infringement of fundamental rights necessarily entailed in a system of data retention and disclosure is kept to the necessary minimum required in a democratic society. As already indicated, consideration of these safeguards is the centerpiece of Chapter 3.

249. Suffice it to say here that the principle of proportionality is also crucial to the operation of a data retention system that has been reduced in scope in compliance with the judgment in *Tele2*. As the ECJ has pointed out in that case, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may be assisted significantly by reliance on modern investigation techniques, this does not in itself justify recourse to the retention of communications data. The necessity for such measures must first be established.

250. Moreover, necessity in this context does not mean that such a system of data retention would simply be useful to national investigatory bodies or constitute an advantageous addition to their existing investigative arsenal. As the Advocate General explained in his Opinion in *Tele2* (at paragraph 209), "*given the requirement of strict necessity, it is imperative that national courts do not simply verify the mere utility of general data retention obligations, but rigorously verify that no other measure or combination of measures, such as the targeted data retention obligation accompanied by other investigatory tools, can be as effective in the fight against serious crime.*"(Emphasis added)

251. As will be seen presently, the net effect of the ECJ's ruling in *Tele2* is that, apart from limiting the scope of the system in the manner described above, the full force of the proportionality principle also applies to all of the operational features of any national system of communications data retention and disclosure.

CHAPTER THREE: OPERATIONAL SAFEGUARDS

INTRODUCTION

The New Landscape

252. It will be recalled that the Terms of Reference countenance the continuance of a statutory scheme for the retention and disclosure of private communications data, citing in this regard the requirement to take account of ''the need for statutory bodies with investigative and/or prosecution powers to have access to data in order to prevent and detect serious crime.'' It will also be recalled that the outer limits of communications data retention systems have been significantly affected by the decision of the ECJ in *Tele2*. Broadly speaking, private traffic and location data may no longer be automatically retained in respect of the public at large without exception or qualification.

253. However, it is important to recognise that*Tele2*also countenanced the continuance of national systems of data retention and disclosure provided they are targeted at a segment or segments of the public (as distinct from the public at large) whose data can be clearly and objectively linked to serious criminal activity or the threat of such activity; and provided retention and disclosure are proportionate responses to those realities (at paragraphs 108-111 of the Judgment). It should also be recognised that there is nothing in *Tele2*that precludes targeted data retention and disclosure – in the sense just described - for the various other purposes sanctioned by Article 15(1) of Directive 2002/58EC: viz., national or state security, defence, and public security.

254. Moreover, the ECJ in that case was at pains to point out – at paragraph 91 of the Judgment - that a national legislative scheme designed along these lines must be configured in accordance with the fundamental rights guaranteed by Articles 7, 8 and 52(1) of the European Charter of Fundamental Rights. In the opinion of the Court, this was essential to ensuring:

- the operational integrity of the system, including the security and confidentiality of communications data during retention periods, and their prompt irreversible destruction following the expiry of such periods (at paragraph 122 of the Judgment);
- that retained data is securely stored within the European Union (at paragraph 114 of the Judgment);
- that retention of communications data is strictly limited to purposes set out exhaustively by Article 15(1) of Directive 2002/58EC (at paragraph 90 of the Judgment);
- that retention and access can be shown to be necessary for the achievement of legitimate statutory purposes (at paragraph 116 of the Judgment);
- that retention and access is proportionate to such purposes (at paragraph 115 of the Judgment);
- that appropriate safeguards for the protection of fundamental rights affected by data retention and disclosure have been installed (at paragraph 117 of the Judgment);
- that these safeguards are given the force of law (at paragraph 94 of the Judgment);
- and, save in cases of verifiable emergency, that access is subject to prior review by a court or independent administrative authority (at paragraph 120 of the Judgment).

255. In what follows, the key provisions of the 2011 Act will be examined in light of these considerations, with special attention being given to the likely shape of a data retention and disclosure system recast in accordance with the new legal landscape sketched now out by the ECJ in *Tele2*.

Principal Frailties of the 2011 Act

256. Recitation of the principal frailties of the 2011 Act provides a useful prelude to the ensuing consideration of necessary safeguards. They include: allowing statutory bodies an effective power of self-certification when making disclosure requests; failure to provide for prior independent authorisation of disclosure requests; failure to adhere to the clear statement principle by permitting undue legislative scatter of the rules governing data retention and disclosure; failure to articulate sufficiently clear objective criteria governing the conditions, circumstances and purposes surrounding data retention and disclosure; failure to provide clear procedures and protocols for the statutory bodies given a right of access to retained data; failure to make provision for the notification of persons affected, either directly or indirectly, by disclosure requests; failure to make appropriate provision for a remedy for wrongful access to retained data; failure to provide for the storage of retained data within the European Union.

DATA MANAGEMENT AND SECURITY

Preliminary

257. Data management and security of retained data is of vital importance in protecting the rights of journalists and persons generally given the vast array of personal data collected and stored during the relevant statutory retention periods by companies in the private section, namely the Service Providers. When accessed by statutory bodies such as the Garda Siochana, it follows that retained data, including data which may contain intimate details concerning a person's private life, will inevitably have a significant level of circulation among investigators within these bodies. Hence the need to provide for high standards in securing and managing the confidentiality of retained data; as well as preventing leakage, misuse or unauthorized access – the need for such standards being both self-evident and a requirement of EU law.

258. There are various stages in the operation of a statutory system governing the retention and disclosure of retained data that are especially important from the point of view of guaranteeing the overall integrity of the system and maintaining public confidence in it. Broadly speaking, these stages comprehend the full array of measures designed to ensure that the vast corpus of private data retained by Service Providers is protected against misuse, abuse and unauthorized access.

These include:

- The collection and storage of data by private communications companies, and the level and type of security attached to these operations
- The identification of the specific bodies or authorities to be granted statutory authorisation to access retained data and the respective statutory purposes for which they are entitled to seek such access;
- The framing of the criteria governing access to retained data, and the definition of key terms involved in their application;
- The point of decision in each individual case, having regard to applicable criteria, as to whether there are sufficient grounds in law for authorising access to retained data;
- The process and procedures to be followed by the body or authority seeking access to retained data;
- The rules and procedures pertaining to the safety and security of personal data following its disclosure to a requesting body or authority, including arrangements for differentiating between data relevant to the purpose for which it had been obtained and information irrelevant thereto;
- The dissemination of personal data to investigators and the like outside the central unit of the authority or body to which retained data has been disclosed, including

arrangements for ensuring that information disclosed is relevant to the purpose for which it has been disclosed, and that its confidentiality is otherwise maintained;

- The arrangements governing the destruction of all data accessed by a body or authority when it is no longer required for the purpose for which it was obtained. (This may arise, for example, when it is found that the personal data contains no useful or relevant information to the purpose for which it had been obtained or after a criminal investigation has concluded with the trial and acquittal of the suspected person).

Retention Periods

259. Section 3 of the 2011 Act sets out the retention periods for which Service Providers are obliged to retain the two categories of communications data to which the Act applies: *viz*., two years for telephone data, and one year for internet data. These were the maximum retention periods permissible under Directive 2006/24. As that Directive has been invalidated, there is now no express provision in EU law dealing with maximum, or for that matter, minimum data retention periods. In the result, provision for data retention periods in any new or amending legislation will have to be calibrated in light of the principle of proportionality. Accordingly, it will not be enough to show that the retention period is likely to be useful or efficacious in respect of the statutory objectives being pursued. Care should also be taken to ensure that, insofar as is practicable, any retention periods selected are objectively justifiable and are no longer than necessary for the purpose of securing those objectives. (**R**).

Service Providers

260. Section 4 of the 2011 Act requires Service Providers to adopt security measures in relation to communications data retained by them in accordance with section 3 of the Act.

261. In summary, section 4 provides that these measures shall be of the same quality and subject to the same security and protection "as those relating to the publicly available

electronic communications service or to the public communications network". The standards implicit in this requirement are not defined. Section 4 goes on to provide that retained data shall be subject to "appropriate technical and organisational measures" to prevent accidental or unlawful destruction or unauthorised or unlawful storage, access or disclosure. The section also provides that the data shall be subject to "appropriate technical and organisational measures" to ensure that they can be accessed by specified authorised persons only.

262. Although the data security requirement imposed on them by section 4 of the 2011 Act is stated in broad, non-specific terms, and leaves a wide margin of discretion as to how it should be interpreted, the Review is satisfied that Service Providers endeavoured to fulfil their data security obligations under the Act in the spirit of section 4. The security measures adopted by Service Providers for this purpose included:

- Providing that the call data recording system automatically streams data (with appropriate filters) into two separate databases - a billing database and a retained communications database, respectively;
- Regular destruction of retained data after the expiry of the statutory period specified in section 3 of the 2011 Act (except for data disclosed under section 6);
- Establishing a small dedicated team of authorised staff to act as a single-point-of-contact within the company to deal with all disclosure requests and court attendance related to same;
- Ensuring that all authorised staff are security vetted;
- Ensuring that all relevant work is carried out in a secure environment where only authorised staff have access to the area where retained data is processed;
- Putting in place a user access management policy to ensure that the requirements of the Data Protection Act are adhered to;

- Conducting annual self-assessments supplemented by audits of data protection systems and procedures;
- Using encryption to ensure secure data transfer; and
- Attaining and maintaining the relevant ISO standards for data security.

263. It should be noted in this regard that the security obligations imposed on Service Providers by section 4(1)(a) to (d) of the 2011 Act are copied verbatim from paragraphs (a) to (d) of Article 7 of Directive 2006/24 to which the 2011 Act gives effect.

264. Article 7imposed on each Member State the obligation to "ensure" that Service Providers "respect, *as a minimum*, the following data security principles ...", going on to state the matters now replicated in section 4(1) of the 2011 Act. Note that the obligations arising under Article 7 are described as principles rather than standards. Note too that the effect of section 4 of the 2011 Act is to preserve the minimalist approach of the Directive to the issue of data security, and to transfer the State's responsibility for implementing the minimalist principles laid down in the Directive directly to Service Providers. Thus paragraphs (b) and (c) of section 4(1) of the 2011 Act simply require Service Providers to secure retained data by subjecting it to "appropriate technical and organisational measures", without mentioning any objective criteria for determining what might be appropriate in this context, let alone adopting specific processes or procedures that must be followed when addressing the issue of data security.

265. This aspect of Article 7 of Directive 2006/24 was heavily criticised by the ECJ in *Digital Rights Ireland*. According to the Court, regarding:

> *"the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the retained data against the risk*

of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that Directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection of and security of data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down."

266. Given that it simply transposes them into Irish law, these observations apply with equal force to the security principles which section 4(1) of the 2011 Act purports to impose on Service Providers in this country.

267. These criticisms might be amplified to the effect that the detailed rules governing data security to which the ECJ alluded, together with the obligations imposed on Service Providers in this regard, should be incorporated into the enactment establishing a data retention and disclosure scheme. This arrangement would help to build public confidence in the system by providing that the strict security standards to be observed by Service Providers have the force of law. (**R**)

268. To say the least, given the legitimate criticisms which the ECJ made of Directive 2006/24, the corresponding section 4 of the 2011 Act must be considered inadequate in respect of the security obligations and standards it seeks to impose on Service Providers. Moreover, the imposition of substantive security obligations based on objective criteria is crucially important for the proper monitoring and supervision of compliance with those obligations by an independent authority. The obligation on the State to impose these standards on Service Providers now arises from Article 4 of Directive 2002/58 from which – as the ECJ pointed out in *Tele2*, at paragraph 122 of the Judgment – there may be no derogation. The Court went on to state:

''Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communication services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organizational measures.''

269. As we have seen, however, the State did not specify data security measures in the 2011 Act. It merely restated the principles which Directive 2006/24 said should be observed in this regard, while at the same time handing responsibility for defining data security standards to private Service Providers without any accompanying rules and safeguards specifically tailored to that end. Bearing in mind that the 2011 Act was designed to establish a system of automatic and indiscriminate data retention affecting the public at large, the approach to data security taken by its progenitors can, at best, be described as nonchalant. In the opinion of the Review, if the State wishes to create a communications database – even one with a reduced footprint in line with the decision in *Tele2* – it must take full responsibility for ensuring that specific rules governing data security are clearly set out, cast in the form of verifiable standards, accompanied by appropriate safeguards, and are understood and applied as such by Service Providers. (**R**)

Factoring in *Tele2*

270. The data security measures identified by the ECJ in *Digital Rights Ireland* have been superseded by the specific standards laid down by that Court in *Tele2*. These are based on the provisions of Article 4 of Directive 2002/58. In *Digital Rights Ireland* the ECJ was referring to standards which must be contained in an EU measure imposing an obligation on Member States to retain data on foot of Directive 2006/24, an obligation that no longer exists since that Directive was invalidated. In contrast,*Tele2* sets out standards for national legislation providing for the retention of communications data as an exceptional measure pursuant to Article 15(1) of Directive 2002/58. There is no longer an obligation on Member States to make provision for a system of communications data retention but if they choose to do so it can only be done by way of an exceptional targeted measure.

271. In consequence, when introducing an exceptional measure on foot of Article 15(1) of Directive 2002/58 Member States must also ensure full compliance with the provisions of the Directive dealing with the security and confidentiality of retained data: viz., Article 4(1) and 4(1)(a). As the ECJ pointed out (at paragraph 122 of the Judgment), those provisions require Member States to ensure that Service Providers take appropriate technical and organisational measures in order to ''guarantee a particularly high level of protection and security'' against unlawful access.

272. As already indicated, this can only be effectively done by enumerating the security standards and procedures with which Service Providers are obliged to comply in national legislation. In order to ensure that they reflect best practice in the information technology industry, these standards and procedures might be drawn up in consultation with the industry. Crucially, they should amount to a set of clearly stated substantive obligations based on objective criteria Service Providers are strictly required to meet, rather than, as at present, a collection of self-imposed measures which Service Providers themselves deem appropriate. In short, legal clarity and detailed obligation on the issue of data security should replace the current system of individualised discretion. (**R**) Legislative provisions designed along these lines need not be overly prescriptive, but they must be coercive in the sense that they promote strict compliance with required standards, and, as will be seen presently, thus facilitate meaningful oversight and review by an independent supervising and monitoring authority. (**R**)

Data Destruction

273. Before considering the general role of an independent body charged with supervising and monitoring data security compliance by Service Providers, the importance of two additional security measures should be considered in the context of promoting the overall integrity of a data retention system, on the one hand, and limiting interference with the fundamental rights necessarily affected by it, on the other.

274. The first of these is the need for a comprehensive requirement to destroy all retained data at the expiry of the relevant statutory retention period, and to ensure that all data retained beyond this point, in accordance with the statutory purposes for which it was originally accessed, is destroyed when no longer required for those purposes. The first part of this requirement is currently met by section 4(1)(d) of the 2011 Act which provides that all retained data shall be destroyed by the Service Provider after a retention period of two years and one month in the case of telephone data, and a period of one year and one month in the case of Internet data.

Spent Data

275. However, that provision makes an exception in respect of data which has been accessed and preserved as a result of a request pursuant to section 6 of the Act – which sets out the terms and conditions governing disclosure requests by the various statutory bodies recognised for that purpose. The settled practice in this regard is for the Service Provider to retain a so-called "golden copy" of data released - for example, to the Gardaí - on foot of a disclosure request, thus providing a basis for verifying its authenticity in the event that this was required in subsequent legal proceedings. In the opinion of the Review, this is a security lacuna that should be closed. Service Providers should be legally obliged to destroy retained data once retention is no longer required for the statutory purposes for which the data were originally released. (**R**)

276. As matters stand, a significant volume of data released pursuant to section 6 would qualify as spent data in this sense. For example, data pertaining to a criminal investigation which has been concluded without prosecution, to an accused who has been prosecuted and acquitted, or to a person perceived to be a serious threat to the security of the state who ceases to be so considered would fall into this category. It should also be noted in this connection that communications data does not pertain exclusively to the individual or individuals in respect of whom the data were originally obtained. In the nature of things, third parties are also affected by the disclosure of retained data, and thus have a legitimate interest in the timely destruction of spent data.

277. It goes without saying that Service Providers can only be expected to destroy spent data when notified by an accessing body that the data in question are no longer required for the statutory purpose for which they were originally obtained. Accordingly, Service Providers should be placed under a statutory obligation to destroy data which has been ''accessed and preserved'' – in the language of section 4(1)(d) – once notified by the accessing body that they are no longer required for their original purpose. (**R**) By virtue of section 2(1)(c) of the Data Protection Act 1988 data controllers are already prohibited from keeping data for longer than legitimate purposes require. However, this provision applies to data controllers generally and does not take account of the specific context of data retention under the 2011 Act. The argument here is for the express inclusion of a provision for the destruction of spent data in the principal enactment governing data retention and disclosure for the specific purpose of fighting serious crime and the other purposes recognized by Article 15(1) of Directive 2002/58. (**R**) Of course, it is for accessing bodies to determine when data no longer serves its original purpose, and their duties in this and related matters are considered in detail below.

Data Storage

278. The second additional security measure is that communications data retained on foot of a statutory obligation should be stored within the State. This follows from the ruling of the ECJ in *Tele2* (at paragraph 122 of the Judgment) that national legislation must make express provision to store retained data within the EU. The 2011 Act fails to provide for this. The Review understands that, although there is no statutory obligation to do so, in practice Service Providers routinely store retained data within the State. However, given that the technological capacity now exists to arrange for data storage outside the State or, indeed, outside the European Union, the risks attendant upon the current regime are obvious. Data storage and access rules in countries outside the EU may not be accompanied by the safeguards now required by EU law.

279. Moreover, it should be borne in mind in this regard that the ECJ ruled in *Tele2* that national authorities are ultimately responsible for ensuring that there are adequate

statutory and other provisions in place to ensure the security of the communications data retained by Service Providers. This involves, *inter alia*, the enforcement of national legal measures in the case of a breach of security and the supervision of Service Providers' compliance with any such measures by an independent national supervisory authority. In these circumstances, in order to facilitate the observance and enforcement of these measures, it is recommended that retained data should be stored within the State. (**R**)

Recommendations on Data Security

280. Provision should be made by legislation for the introduction of substantive security measures, including standards and procedures based on objective criteria, to be observed by Service Providers so as to ensure a particularly high level of protection and security of retained data against the risk of abuse and unlawful access or use. (**R**) The security measures which Service Providers are required to implement should be clearly stated in the principal enactment governing data retention and disclosure for specified statutory purposes. (**R**) In addition to their existing obligations to destroy data at the expiry of retention periods, Service Providers should be placed under a statutory duty to destroy spent data, i.e., data which has been "accessed and preserved" but in respect of which the accessing body has given notice that the data in question are no longer needed for statutory purposes. (**R**)

281. Legislation should specify that retained data must be stored in Ireland, thus ensuring that it is secured and that access to it is limited in accordance with the relevant criteria and safeguards laid down in Irish law. (**R**)

Independent Supervisory Authority

282. The lack of a sufficiently robust legal basis for periodically monitoring and auditing the quality and effectiveness of the security measures adopted by Service Providers has already been mentioned. In this connection Article 9 of Directive 2006/24/EC imposed an obligation on Member States to designate "one or more public authorities" to be

responsible for "monitoring" the application of security provisions adopted pursuant to Article 7 of the Directive, while at the same time giving them the option of assigning this role to national bodies already charged with general responsibility for data protection. Although that Directive no longer applies, as explained hereunder Article 9 embodied a fundamental requirement of EU law on independent monitoring of data security obligations.

283. It will be recalled that section 4(2) of the 2011 Act sought to give effect to this obligation by naming the Data Protection Commissioner as the relevant designated national supervisory authority for overall monitoring of data security. As already indicated, the allocation of responsibility to the Data Protection Commissioner by section 4(2) was done in a perfunctory and inadequate manner, not least because no attempt was made to define the Commissioner's supervisory powers or to specify the criteria against which security compliance by Service Providers was to be measured having regard to the nature of a statutory system of retained communications data.

284. Admittedly, the Data Protection Acts confer a range of powers and responsibilities on the Data Protection Commissioner which apply to data generally, including data retained under the 2011 Act. These powers and responsibilities are set to be expanded in line with the provisions of General Data Protection Regulation 2016/679/EU and Directive 2016/680/EC on the processing of data in connection with the prevention and investigation of crime, both of which will come into force in 2018.

285. Whether a more clearly defined oversight role in regard to the security of retained communications data should be conferred on the Data Protection Commissioner, or whether it might be better discharged by another specialist body properly resourced for that purpose, is a matter of policy choice. The crucial issue is to ensure that the duties assigned to an independent supervisory body are clearly stated in legislation, that sufficient resources (including specialist resources) are provided, and that the supervisory powers and sanctions essential to the discharge of these duties are both substantive and effective. As the ECJ pointed out in *Tele2* (at paragraph 123 of the Judgment), meaningful oversight

in the matter of the security of retained communications data entails ''review, by an independent authority, of compliance with the level of protection guaranteed by EU law''; citing in this regard Article 8(3) of the European Charter of Fundamental Rights as establishing ''an essential element of respect for the protection of individuals in relation to the processing of personal data.'

286. In short, while the imposition of clearly stated objective standards on Service Providers is a necessary condition of data security, it is not a sufficient condition. Given the importance attached to the issue by European law and jurisprudence, national legislation must also provide for a robust form of monitoring and supervision of Service Providers by an independent authority with a clearly defined role and expressly associated powers and duties.[29] Providing the necessary resources, including expert personnel, for such effective monitoring and supervision is essential. (**R**)

287. Such a body should be required to review all security and related measures put in place by Service Providers for the purpose of complying with any relevant statutory obligation. It should also have the power to give directions concerning procedures and protocols which it deems should be adopted by Service Providers for that purpose. (**R**) Clearly, there is a need for detailed rules governing the internal processes and procedure to be followed by Service Providers when handling retained data. These include rules and protocols on the personnel designated to access retained data, either in response to an official data request or for the purposes of data management or record keeping or any other lawful purpose. (**R**) Measures are also required to prevent breaches of security, and, where such breaches occur, to facilitate detection of improper or unlawful access both from within and/or outside Service Providers. In addition, protocols will be required for reporting security breaches to the independent supervisory authority. (**R**)

[29] United Nations Larue Report, council of Europe Resolutions, the ECJ, the ECtHR and national courts.

288. The primary recommendation is that there be a designated independent authority - the Data Protection Commissioner or another independent authority - with defined powers and obligations, and appropriate resources and expertise, charged with monitoring the conduct of data security by Service Providers. This body's statutory brief should include the preparation of an annual review of Service Providers' compliance with their security obligations in respect of retained private communications data.**(R)**

289. In order to facilitate the role of an independent monitoring authority Service Providers should be required to prepare (ideally in consultation with the designated independent authority) a Compliance Statement describing and explaining in detail the security measures (including procedures and protocols) which they have put in place with the aim of fulfilling all the elements of their statutory obligations. **(R)** This Statement should be updated or amended when any changes in those security measures occur. In any event, it should be reviewed by the Service Providers themselves on an annual basis. The Compliance Statement when first drawn up, and upon any subsequent amendment thereto, should be furnished to the independent authority designated to monitor observance by Service Providers of their statutory obligations in this regard. As a matter of course, the current extant version of the Compliance Statement should be sent annually to the designated authority. (**R**)

290. These Statements should be used as a set of reference points by the independent authority when reviewing the practical measures needed to ensure compliance by Service Providers with the level of security required by statute. They should also be used to guide oversight and, where necessary, investigation by the independent authority in the matter of security compliance by Service Providers. (**R**)

291. It should be noted that preparation of a Compliance Statement of the type being recommended here would not place an undue burden on Service Providers. In essence what is being proposed is a formal extension of current practice: viz., the preparation of a comprehensive written document setting out the measures (many of which have already

been adopted in compliance with section 4 of the 2011 Act) put in place to guarantee the security of retained data in line with statutory requirements.

Recommendations on Independent Monitoring Authority

292. A supervisory authority, whether it be the Data Protection Commission or another independent authority, should be expressly designated as a monitoring authority in respect of security compliance by Service Providers in the matter of retained data. (**R**) The authority should be given defined powers and duties, and endowed with appropriate expertise. (**R**) Its duties should include periodically monitoring observance by Service Providers of their obligations regarding the security of communications data which they are obliged to retain. (**R**) The authority should also be allocated the power to give directions to Service Providers concerning procedures and protocols to be observed for security purposes. These powers and functions should be accompanied by all necessary resources. (**R**)

293. Service Providers should be required to draw up a Compliance Statement describing and explaining in detail the security measures (including procedures and protocols) which they have put in place for the purpose of fulfilling all elements of their statutory obligations in respect of data security including protection against unlawful or unauthorised access. (**R**) A copy of the Compliance Statement should be furnished annually to the supervising authority and any interim amendments or updating thereto should be notified to that authority as and when they are introduced. (**R**)

ACCESS TO DATA

Role of Service Providers

294. The role of Service Providers is key to the security and integrity of a properly regulated system of communications data retention and disclosure. Even in a system reduced in scope in line with the landmark ruling in *Tele2*, Service Providers will continue

to act as custodians and gatekeepers of communications data lawfully retained in connection with the prevention and prosecution of serious crime and other lawful purposes. In the result, they will continue to play an important part in the process whereby retained data may be accessed for specified statutory purposes by recognised statutory bodies. Accordingly, it is essential that their powers and duties in this regard are properly and effectively regulated. The Act of 2011 seeks to do this in a variety of ways and one of the tasks of the Review is to examine these strategies in the light of established principles and standards concerning such matters.

295. In essence the approach taken by the 2011 Act is to prohibit access to retained data by Service Providers save for the purpose of facilitating disclosure requests by recognised statutory bodies; and to confine the basis for disclosure requests to a limited number of specified statutory purposes.

296. Thus, section 5 of the 2011 Act provides that a Service Provider shall not access data retained in accordance with section 3 except--

- at the request of a person to whom the data relate;
- for the purpose of complying with a disclosure request. These are requests by the relevant statutory bodies referred to in section 6, namely:
- the Garda Síochána,
- the Defence Forces,
- an officer of the Revenue Commissioners,
- the Competition and Consumer Protection Commission, and
- by virtue of s. 98 of the Garda Síochána Act, 2005 the Garda Síochána Ombudsman Commission];
- In accordance with a court Order; or

- as may be authorised by the Data Protection Commissioner.

Persons to Whom Data Relate

297. The role of Service Providers in facilitating disclosure requests by statutory bodies is considered in detail later in the Chapter. Suffice it to notice here that their role in facilitating requests by ''a person to whom the data relate,'' as set out in section 5(a) of the 2011 Act, is deserving of comment. As currently drafted, it is unclear whether section 5(a) includes the recipient of a communication as well as the person who made contact with the recipient. Plainly it includes the person making the communication, even if it could be argued that the person who receives or is a party to the communication is also ''a person to whom the [resultant transactional] data relate.''

298. Be that as it may, there is a risk that the provision could be used to facilitate the disclosure of private data in circumstances not contemplated either by the long title to the 2011 Act or by the general scheme for the disclosure of private data set out in the body of the Act. As already indicated, both the long title and the main provisions in section 6 link disclosure explicitly to the nominated purposes of preventing serious crime, safeguarding the security of the state, and saving human life. In contrast, section 5(a) arguably countenances disclosure in circumstances unconnected to such purposes.

299. For example, section 5(a) might be relied on where a party to legal proceedings was the subject of a court order for the production of retained communications data relevant to those proceedings but in no way connected to the aforementioned purposes specified in the 2011 Act. Compelling disclosure of historical private communications data, available only by virtue of a statutory retention scheme, could be in breach of the right to privacy under Article 8 of the European Charter of Fundamental Rights; and, in the case of journalists, could seriously compromise the confidentiality of their journalistic sources. In this connection, it should be borne in mind that a journalist whose sources came to light in these circumstances need not necessarily have been the instigator of the retained, and

then subsequently disclosed, communication. As already indicated, he or she may have been the recipient of a communication or series of communications initiated by another.

300. Given the holding in*Tele2* (at paragraph 115 of the Judgment) that access to retained data must be strictly linked to the statutory purpose for which it was originally retained, this problem should be catered for in any amending legislation designed to incorporate the requirements of European law in the matter of data retention and disclosure.

301. In particular, more precise provision should be made concerning the circumstances and purposes for which a person may personally request, and therefore be exposed to being compelled to request, disclosure of their personal communications data history. (**R**) Naturally, this should be done in full cognizance of the requirements of the General Data Protection Regulation (EU) 2016/679and Directive 2016/680/EC on processing data in the context of criminal investigations and prosecutions.

Generally Applicable Measures

302. Disclosure requests – as introduced in section 5(1)(b) and provided for in section 6 of the 2011 Act - are the most frequently used means of accessing retained communications data. Apart from the rules and procedures that might be deemed specific to particular statutory bodies when using disclosure requests, there are several generally applicable or overarching requirements as to the safeguards which should apply to all disclosure requests, irrespective of their source. First, disclosure requests should be evaluated in accordance with the principle of proportionality. Generally speaking, proportionality in this context would include consideration of the availability of alternative, less intrusive action, as well as the possibility of limiting the scope of a disclosure request, the type and volume of data requested, and the timeframe covered by the request. Moreover, there is an overriding consideration– articulated by the ECJ in *Tele2* at paragraph 116 the Judgment - to the effect that a disclosure request that cannot be shown to be strictly necessary for the achievement of a specified statutory objective must be

deemed to be disproportionate, and thus to constitute an unwarranted intrusion on the right to data privacy guaranteed by Article 7 and 8 of the EU Charter of Fundamental Rights. (**R**)

303. Second, all disclosure requests should be subject to prior authorisation by a judge or an independent authority. (**R**) Where the purpose of a disclosure request is the identification of a journalist's sources, prior authorization should be sought from a judge of the High Court. (**R**)

304. Third, applications for prior authorisation should be in the form of a statutory declaration containing all the essential information pertaining to the basis for the disclosure request and the statutory purpose for which the request is being made.(**R**)

305. Fourth, In the case of disclosure requests for the purpose of identifying a journalist's sources, this purpose should be expressly stated without prejudice to other details to be included in an application for authorisation to make a disclosure request. (**R**)

306. Fifth, only designated officers or members of the statutory bodies in question should be authorised to approve and submit an application for authority to make a disclosure request. (**R**)

307. Sixth, personnel designated by the relevant statutory bodies to decide whether an application for prior authorisation should be submitted should receive essential training in the importance of the right to privacy and the substantive meaning and effect of the principle of proportionality when deciding whether communications data should be accessed in a particular case; as well as instruction on the safeguards to be observed in ensuring both the security of the data and its non-disclosure for purposes or to personnel other than those strictly concerned with the statutory basis for the disclosure request. (**R**)

308. Seventh, provision should also be made for the imposition of sanctions in respect of wrongful access to private data, including criminal sanctions in the event of intentional

or reckless wrongful access. (**R**) It will be recalled that the 2011 Act is silent in this regard, notwithstanding the presence of a provision on sanctions in the originating Directive.

309. Finally, the following matters might also be included under the rubric of overarching provisions relevant to the powers of access enjoyed by statutory bodies:

- the imposition of a general duty to submit an annual report to the relevant minister;
- the introduction of a requirement to publish these reports or at least a summary thereof compiled by the Minister for Justice and Equality (as matters stand the Minister is merely obliged to furnish a composite report to the EU Commission);
- standardisation of the document, affidavit or statutory declaration forming the basis of an application to a judge or an independent authority for authorisation to make a disclosure request;
- the imposition of a general duty on statutory bodies to destroy data which are no longer required for their respective statutory purposes. (**R**)

Statutory Cohesion

310. Given the grave risks associated with access to private data, both for citizens and journalists alike, and the concomitant need to build public confidence in an appropriately calibrated system of controlled access, serious attention should be given to the question of statutory cohesion in the matter of data retention and disclosure. In summary, it is recommended that the rules governing the retention and disclosure of private communications data should be contained in a single statutory enactment including regulations made thereunder. (**R**) In line with the principle of foreseeability emphasised in the case law of the ECtHR, these rules should be stated in clear, accessible language, thus enabling affected individuals to adjust their conduct accordingly. (**R**) The Act should deal exhaustively with the various avenues of access to private data permissible in Irish law; and should specify all of the bodies entitled to seek such access. (**R**) Moreover, any subsequent

alteration in arrangements governing access to retained data should be done by way of amendment to the principal enactment. (**R**) As matters stand, none of these conditions is met by the 2011 Act.

Recommendation on Statutory Cohesion

311. Any new or amending Act should be drafted so as to identify all of the bodies or persons who may have a right of access, even if through a court application, to data such as that retained under section 3 of the current 2011 Act. An express provision should be contained in the Act stating that only persons or bodies designated in the Act may have access to such data for the purposes and on the basis of an application of a kind specified in the Act. Any grant of a right of access or an amendment to these matters subsequently arising should be done only by way of express amendment to the principal Act. (**R**) The provisions of the Act should adhere rigorously to the principle of foreseeability (as described in the jurisprudence of the ECtHR summarised in this Chapter). (**R**)

Statutory Bodies Generally

312. The role of Service Providers in facilitating disclosure requests by statutory bodies, the most frequently used avenue of access to private communications data, has already been mentioned. As we have seen, section 5 of the 2011 Act permits Service Providers to access private data on foot of such requests; while section 6 sets out the terms and conditions with which disclosure requests must comply for the purpose of securing access to private data, and, with the notable exception of GSOC, identifies the bodies entitled to issue disclosure requests to Service Providers. As previously indicated, GSOC also makes disclosure requests pursuant to section 6 by relying on powers vested in it by section 98 of the Garda Síochána Act 2005.

313. It will be recalled in this connection that the ECJ stated in *Tele2* stated (at paragraph 118 of the Judgment) ‘’that national legislation must lay down the substantive

and procedural conditions governing the access of the competent national authorities to the retained data…''

314. The first statutory body identified in section 6 is the Garda Síochána. Section 6(1) circumscribes that body's right of access as follows: a disclosure request must be made by -

(a) an officer not below the rank of Chief Superintendent;

(b) that member must be satisfied that the data are required for

(c) the prevention, detection, investigation or prosecution of a serious offence;

(d) the safeguarding of the security of the State; or

(e) the saving of human life.

315. As regards (a) this means in principle that every Chief Superintendent in the country, and, indeed, any officer above that rank, may make a request for access to the private data of any individual once he or she is satisfied that such information is required for one of the specified purposes. In practice, this is not how the disclosure request system is operated by the Garda Síochána. On the contrary, there is a dedicated and structured unit at Garda Headquarters with exclusive administrative responsibility for processing and submitting disclosure requests to Service Providers. A Chief Superintendent has been assigned as head of that unit, and that person is responsible for approving and making the final decision on the submission of a disclosure request to a Service Provider for the purposes of the section. In addition, provision has been made for the exercise of that decision-making authority by an alternatively designated Chief Superintendent when the original assignee is not available.

316. In the opinion of the Review, these essentially administrative arrangements should be supplemented by a formal legal requirement that the designation of the officer responsible for issuing disclosure requests, including that of his or her nominated alternative, should be made by the Garda Commissioner. (**R**) This would give statutory force to what has proved to be an effective arrangement for the preparation of disclosure

requests, and would help to strengthen the ''single-point-of-contact'' principle underpinning that arrangement. The essence of this principle is that the number of personnel involved in the process of preparing disclosure requests should be kept to a necessary minimum, on the grounds that this fosters greater coherence and higher standards of decision-making than would be possible in a system where responsibility is more widely allocated, while at the same providing an important safeguard against the risk of inappropriate access. Statutory recognition of the ''single-point-of-contact'' principle in this context would also help to increase public confidence in the overall integrity of a system of data retention and disclosure.

317. Statutory recognition should also be given to the ''single-point-of-contact'' principle in respect of the other bodies – including GSOC - entitled to make disclosure requests pursuant to section 6 of the 2011 Act.(**R**) As in the case of the Garda Síochána, all of the other affected bodies, including GSOC, currently apply the ''single-point-of-contact'' principle as a matter of administrative practice. Incorporating the principle in legislation would thus give legal effect to an important convergence of practice and procedure among the bodies charged with the secure management of disclosure requests.

318. Several additional practices and protocols currently operated by the statutory bodies entitled to make disclosure requests pursuant to section 6should also be cast in a form that has the force of law, whether by statute or statutory regulation. These include the issuing of guidelines and instructions as to the proper content of applications submitted to the member or officer charged with responsibility for making disclosure requests within the various statutory bodies. Broadly speaking, these guidelines and instructions seek to promote best practice in the area of data protection and minimal intrusion on personal rights and freedoms in the operation of the system of disclosure requests enshrined in section 6. (**R**)

319. For example, the Garda Síochána Headquarters Directives issued in 2013prescribe the procedures for initiating disclosure requests. Members of the Garda Síochána who wish to obtain communications data encompassed by section 6 of the 2011 Act must

submit an application to the ''single-point-of-contact'', the Detective Chief Superintendent of Security and Intelligence(DCSSI), who is supported by the Garda Communications Liaison Unit (TLU). All disclosure requests issued to communications Service Providers must be approved by and emanate from the DCSSI. In contrast, the TLU does not carry out any investigative function but merely serves as a conduit between the communications Service Providers and the Garda Síochána. Applications from the Garda Síochána to the TLU for the making of a disclosure request must be recommended by a superintendent or an inspector acting as a superintendent. The relevant Headquarters Directives require that the application to the TLU must contain sufficient detail of the matter under investigation to enable the TLU to make an informed decision. For example, Headquarters Directive 24 of 2013 makes it clear that all applications should include the following:

- Precise details of the offence under investigation, including the relevant statutory provision/s and penalties;
- Information on the source of the telephony or internet number – the phone number, IMEI number, SIM card number, IP address, account name etc. – at the centre of the investigation;
- Details of the relevance to the investigation of the data requested;
- A statement of the objective to be achieved and how this objective is to be realised. For example, if it is intended that the identification of numbers and subscriber details will be followed up by interview with the person or persons whose metadata is being sought.

320. The Garda Síochána Headquarters Directives also require that applications must have regard to the issues of relevance, necessity and proportionality in accordance with the European Convention on Human Rights. Prior to submitting initial requests to the Chief Superintendent, the TLU staff scrutinise applications to ensure compliance with these and other relevant criteria. The TLU will often request further information before submitting an application to the DCSSI. Approximately 60% of applications were returned to sender

on this basis in 2014. Once satisfied that the application meets the relevant requirements of the legislation and that sufficient information has been supplied, the TLU forwards the application for consideration by the DCSSI. Finally, if that officer is satisfied that the requirements of the legislation have been met and that the disclosure sought is necessary and proportionate he or she will make a formal disclosure request to the relevant communications Service Provider.

321. The Review has learned that similar controls are in place in the other statutory authorities. Moreover, all of the statutory bodies consulted stated a general preference for using disclosure requests as a last resort, to be employed only where other, less intrusive, investigative options - such as telephone directories and web pages - are unavailing. In addition, the permissive reach of section 6 notwithstanding, most statutory bodies expressed a preference for initially limiting the scope of a disclosure request unless and until a compelling case for broadening it out has been established. For example, investigating officers are advised to confine their initial investigations to telephone numbers called from or called to a suspect's device; and to progress to requests for subscriber details if and only if there is reason to believe – perhaps because of the timing of a particular call – that this is relevant to the objectives of the investigation.

322. All of the foregoing internal arrangements are non-statutory. Accordingly, it is recommended that enforceable regulatory provision should be made for arrangements of this kind as they limit the scope for abusing the intrusive provisions of the 2011 Act and give formal recognition to the key element of quality control in the preparation of disclosure requests within the various statutory bodies prior to the final submission of a disclosure request. The broad principles and policies governing internal controls should be set out in primary legislation. (**R**)

323. More detailed provision could also be made for individual statutory bodies, either by way of statutory instruments made by the relevant Minister, or by way of internal guidelines which would be subject, in accordance with statute, to approval by the relevant Minister or by a tribunal established to oversee various aspects of the operation of data

disclosure powers. Members of staff of the various statutory bodies should be given formal instruction on how the issue of proportionality should be assessed so as to ensure that it is seen and understood as matter of fundamental rights and obligations and not simply as an incidental question of administrative efficiency. Such instruction should encompass the preparation and dissemination of a formal document detailing the aforementioned matters. (**R**)

324. The Criminal Justice (Surveillance) Act 2009 affords an interesting example an example of how a test purporting to balance fundamental rights and the use of intrusive powers can be set in legislation. Section 4(5) of the 2009 Act provides as follows:

> *"A superior office who makes an application under subsection (1), (2), (3) or (4) shall also have reasonable grounds for believing that the surveillance being sought to be authorised is:*
>
> > *(a) the least intrusive means available, having regard to its objectives and other relevant considerations,*
> >
> > *(b) proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and*
> >
> > *(c) of a duration that is reasonably required to achieve its objectives.''*

Recommendations on Statutory Bodies Generally

325. Existing legislation should be amended so as to provide that disclosure requests on behalf of each statutory authority may only be made by a limited set of Chief Superintendents, Colonels, Principal Officers etc. who have been designated by the Garda Commissioner, Chairman of the Revenue Commissioners, Chief of Staff of the Defence Forces, to exercise that function for the purposes of the Act. (**R**) In the cases of the Competition and Consumer Protection Commission and GSOC, the legislation already limits

the power to make disclosure requests members of the respective Commissions. This limitation should be maintained in any amended legislation, with an additional requirement that a maximum of three of the six potential members of the Competition and Consumer Protection Commission may be designated for the purpose of making disclosure requests. (**R**) It should be a requirement of legislation (whether primary or secondary) that investigators in all of the relevant statutory bodies should, as part of the process of submitting a proposal to a designated officer that a disclosure request be made set out:

- Details of the specific offence under investigation, including the relevant statutory provisions and penalties, and the facts or circumstances showing that the request relates to a serious criminal offence or a serious threat to national security.
- The relevance to the investigation of the data being requested.
- The objective sought to be achieved by obtaining disclosure of the data and how this objective is to be realised.
- Whether any attempt has been made to attain the objectives of the investigation by less intrusive means. (**R**)

326. It should be a requirement of legislation that investigating officers and designated officers of the statutory bodies should be instructed (such instruction to include a formal document) on how proportionality is to be assessed so as to ensure that it is seen and understood as matter of fundamental rights and obligations and not merely as a question of efficiency. In the case of the Defence Force, this requirement should apply both to the officers designated to apply for disclosure requests, and to members who may apply to those officers for the purpose of initiating such requests. (**R**)

327. It should be a formal requirement of the legislation that a designated officer should have reasonable grounds to believe that the disclosure of retained communications data relating to the investigation of serious offences, safeguarding the security of the State or saving a human life is:

- the least intrusive means available, having regard to the objectives for which it is being sought and other relevant considerations,
- proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and
- of an extent that is reasonably required to achieve its objectives. (**R**)

328. Legislation (primary or secondary) should specify the form of document, affidavit or statutory declaration, which would provide the basis of either an application to a judge or to an independent authority, for authorisation to make a disclosure request, including the essential elements of same. (**R**)Without prejudice to specific recommendations as to its contents, the application should contain sufficient information and reasons to satisfy the judicial or independent authority that the granting of the request meets all the requirements of the law, particularly the principle of proportionality. (**R**) (This requirement should apply to all such applications by statutory bodies).

329. Each statutory body should be required by legislation to destroy data when no longer required for the purpose for which it was obtained. (**R**)

330. Each statutory authority should have a statutory duty to report annually on the performance of its obligations, functions and powers under the legislation analogous to the existing provisions. (**R**)

331. Legislation should require the publication of such reports or a summary thereof compiled by the Minister for Justice and Equality

Rights to Notification and Judicial Remedy

332. A statutory body which seeks and obtains access to retained communications data should be required to notify the person or persons affected as soon as such notification is no longer liable to jeopardise the investigations or purpose for which access was granted. Express provision should also be made in any amending data retention legislation to ensure

that an appropriate judicial remedy is available to every person whose rights have been wrongfully infringed arising from access to, use or processing of, retained data.

333. The ECJ made express reference to these requirements in *Tele2* (at paragraph 121 of the Judgment):

> *"Likewise, the competent national authorities to whom access to retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact necessary to enable persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of directive 95/46, where their rights have been infringed."*

334. Article 22, Chapter III (on Judicial Remedies, Liability and Sanctions) of Directive 95/46 provides:

> *"Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by national law applicable to the processing in question."*

335. Moreover, Article 23 (Chapter III) of Data Protection Directive 95/46 provides that

> *"Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage."*

336. Accordingly, it is recommended that legislation enjoining the obligatory retention and disclosure of communications data should provide an appropriate judicial remedy for any wrongful breach of an individual's rights, including fundamental rights, as a result of the operation of the system. (**R**) In the opinion of the Review, neither section 7 of the Data Protection Acts, 1988 – 2003 nor Regulation 16(2) of S.I. No. 336/2011 (Privacy and Electronic Communications Regulations) are sufficient to satisfy this objective. The former imposes a liability for a breach of a duty of care on data controllers and processors in quite limited circumstances. It does not provide for a sufficiently complete judicial remedy for breach of fundamental rights due to wrongful access or use of retained data. Similarly, Regulation 16(2)entitles a person who suffers loss or damage as a result of a contravention of any of the relevant Regulations to compensation from the person who caused that loss and damage; this has been interpreted by the High Court as entitling a claimant only to compensation for damage actually suffered, and not for breach of rights *per se: Collins v FBD* [2013] IEHC 137.

337. In the result, bearing in mind the coercive character of a data retention system, and the concomitant risk to fundamental rights associated with it, it is recommended that the statute establishing such a system should expressly provide for an appropriate judicial remedy and associated procedures for breaches of rights, including fundamental rights, occasioned by its operation.**(R)**

338. The foregoing recommendation may be reviewed in the light of any form of equivalent judicial remedy which may be provided for when the General Data Protection Regulation comes into force in 2018.

Need for Punitive Sanctions

339. Finally, it is of fundamental importance that the essential rules, principles and safeguards governing the operation of a system of data retention and disclosure have the force of law. Moreover, if this crucial objective is to be achieved, it follows that the aforementioned rules, principles and safeguards should be backed by punitive sanctions

that can be imposed in the event of violation. Surprisingly, the 2011 Act made no provision in this regard, despite the fact that it was enacted, inter alia, to give effect to Directive 2006/24, Article 13.2 of which provided as follows:

> *"Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of data retained in accordance with, this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive."*

340. Moreover, as the ECJ pointed out in *Tele2*, Article 24 (Chapter III) of Directive 95/46 is also applicable in this connection:

> *"The Member State shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall particularly lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive."*

341. Moreover, in order to have the force of law a legal regime must be backed by sanctions. In the result, a system of communications data retention and disclosure purporting to be regulated in accordance with law must make due provision for punishing those who flout its regulations. Otherwise the coercive force of the rules governing the operation of the system would be gravely diluted. As punitive sanctions are normally the exclusive province of the criminal law in Irish law, it follows that the criminal law is the appropriate means for sanctioning conscious or reckless breach of the rules governing data retention and disclosure. Such breaches should be treated as criminal offences, and the penalties attached thereto should be sufficiently severe so as to ensure that they are effective, proportionate and dissuasive. **(R)**

Serious Offence Criterion

342. It will be recalled that the purposes for which the Garda Síochána may apply for a disclosure request are specified in section 6 of the 2011 Act; and that those purposes are confined by section 6(1) of the Act to the prevention, detection, investigation or prosecution of a serious offence; the safeguarding of the security of the State; and the saving of human life, respectively. In the opinion of the Review, it is self-evident that pursuit of the first of these purposes – the prevention, detection, investigation or prosecution of a serious offence – is a matter of legitimate public interest. The Review is also satisfied that a system of disclosure requests designed to facilitate that purpose, provided it is accompanied by a set of safeguards which limit its impact on fundamental rights to what is necessary and proportionate in the circumstances, is also in the public interest.

343. Clearly, confining disclosure requests to data connected to serious criminal offences is a crucial safeguard in this context, not least because this is a specific requirement of European law. Although mindful of the philosophical difficulties inherent in defining the notion of a serious offence, the Review is satisfied that the approach adopted in the Interpretation section of the 2011 Act, which defines a serious offence as ''an offence punishable by imprisonment for a term of five years or more'', establishes an appropriate threshold in this regard. In the opinion of the Review, it is sufficiently restrictive bearing in mind the highly intrusive nature of a regime of disclosure requests(even when refashioned in accordance with the recommendations set out in this Review); and sufficiently elevated to chime with the companion purposes for which the Garda Síochána are entitled to make disclosure requests pursuant to section 6(1): viz., the safeguarding of the security of the state and the saving of human life.

344. Finally, although the offence on which it is predicated must be a serious offence within the meaning of section 1 of the 20011 Act, it should be remembered that this is not in itself a sufficient condition for acceding to a disclosure request. As the ECJ made clear in *Tele2* (at paragraphs 115-116 of the Judgment), access to retained communications data

must also be shown to be strictly necessary and proportionate in light of the object for which it is being sought. In other words, a disclosure request based on the investigation of a serious offence must also satisfy these conditions. In this regard, it must also be borne in mind that a disclosure request must show that the investigation involves a serious offence *in substance*, not merely one which attracts a punishment of 5 years' imprisonment.

Saving Human Life Criterion

345. As already indicated, the Garda Síochána are also entitled to make disclosure requests for the purposes of safeguarding the security of the state and saving human life, respectively. Disclosure requests for the purpose of safeguarding the security of the state may also be made by the Defence Force; and are considered in the ensuing section.

346. In contrast, the entitlement to make disclosure requests for the purpose of saving human life is unique to the Garda Síochána. Like the previous rubric of disclosure requests for the purpose of fighting serious crime, the Review is satisfied that provision for disclosure requests for the purpose of saving human life is also in the public interest. In the opinion of the Review, this conclusion is self-evident. There is a clear social value or utility to providing for limited data disclosure where there is a risk to human life - for example, by way of assisting in the search for a missing person who may have wandered away from a nursing home or residential facility, and whose life, perhaps because of a medical or psychological condition, may be in danger as a result. It goes without saying that access to location data linked to a missing person's mobile telephone in these circumstances might be crucial to saving that person's life. Similar considerations might be said to apply to a search for a young or vulnerable person who has been reported as missing and whose whereabouts are unknown. The extent of the retained data sought should, in all cases, be proportionate to the object being pursued.

347. A number of additional points deserve to be mentioned in connection with this rubric. First, consideration might usefully be given in amending legislation to ensuring expeditious access to retained data for the purpose of saving human life. In the nature of

things, undue formality in processing disclosure requests under this rubric may defeat the purpose for which they are intended. Second, amending legislation might also consider broadening the scope of the rubric to include the risk that a person's health or personal safety may be in serious jeopardy. In short, the requirement that a person's life must be at risk may set too high a bar in this regard. Third, however defined, the serious risk to life on which the disclosure request is based should be real and proximate. A statutory requirement to this effect would help to confine the rubric to cases of genuine emergency, while excluding cases where the risk in question was remote or purely speculative.

348. Finally, it should be borne in mind that, as currently drafted, the criterion of saving human life is very broadly drawn, with no obvious reference point against which its application can be gauged; unlike its companion criterion of investigating and prosecuting crime, it is not tied to a set of precisely specified activities in the sphere of law enforcement. On the contrary, it may be said to confer undue discretion on the police authorities, and thus to be vulnerable to abuse by them. Accordingly, the Review is of the opinion that efforts should be made to ensure that the rubric of saving human life is not misused as an umbrella for disclosure requests – for example, originating in the course of a criminal investigation - with no more than remote or speculative links with the objective of saving human life. In part, this problem can be ameliorated by introducing the statutory amendment canvassed in the preceding paragraph. But it should also be addressed when framing the protocols to be followed by statutory bodies when preparing disclosure requests.

Recommendation Regarding Saving Human Life

349. The statutory criterion for seeking disclosure of data for the purpose of saving human life should be strengthened by circumscribing it such that, at the very least, it can only be relied upon where there is a real and proximate risk to the life of a person or persons. (**R**)

Access for Mutual International Assistance

350. It will be recalled that the Garda Síochána also make disclosure requests on foot of the provisions of the Criminal Justice (Mutual Assistance) Act 2008. As already pointed out in the concluding section of Chapter 1, the 2008 Act forms part of the legislative framework governing access to retained communications data held by Service Providers. Broadly speaking, the purpose of the 2008 Act is to give effect to certain international agreements between the state and other states relating to mutual assistance in criminal matters. Accordingly, section 75 of the 2008 Act provides for access to retained communications data for the purpose of complying with a request for such data by a foreign police or security agency. The procedure in outline is as follows. A member of the Garda Síochána not below the rank of inspector, on the direction of the Minister for Justice*, may apply to a designated judge* of the District Court for an order requiring a Service Provider to furnish retained data in respect of a particular person over a specified period. Once the procedures governing application to the District Court have been complied with, the judge in effect has no discretion to refuse the application. Moreover, by virtue of section 5 of the 2011 Act, Service Providers in turn are required to grant access to retained data in accordance with a court order thus obtained.

351. The key issue for the Review is that the 2008 Act provides a statutory means of access to retained communications data, including the communications data of journalists, by foreign authorities. Although this data is retained by Service Providers pursuant to their obligations under the 2011 Act, there is no express provision in that Act for access to such data by or for the benefit of foreign authorities. Accordingly, as an absolute minimum, the Review is of the opinion that access to retained data of the kind facilitated by the 2008 Act should be subject to the normal criteria governing access by statutory bodies, not only as currently laid down in the 2011 Act but in any amending legislation. Moreover, access to retained communications data should be governed by and accord with appropriate safeguards for the protection of fundamental rights and freedoms. These safeguards –as

enumerated in this Chapter - derive principally from those identified by the ECJ in *Tele2* and the State's obligations under the European Convention on Human Rights. (**R**).

Safeguarding Security of the State

352. It will be recalled that both the Garda Síochána and the Defence Force are entitled to seek disclosure of retained data for the purpose of safeguarding the security of the State. Once again the Review is satisfied that this arrangement is, broadly speaking, in the public interest; both of these bodies have a legitimate role in the defence of the vital institutions of the State and the preservation of public security more generally. However, the Review is of the opinion that the rubric of defending the security of the State is too broadly drawn as it provides what is in effect an open-textured criterion for accessing private communications data in circumstances where there may be no more than a purely theoretical or speculative risk to the security of the State.

353. Nor is it dispositive that, as previously indicated, the internal administration of the rubric by the Garda Síochána and the Defence Force is designed to ensure that disclosure requests made pursuant to it are in strict compliance with the statutory purposes contemplated by subsections 6(1)(b) and 6(2), respectively, of the 2011 Act. Estimable though these administrative arrangements are, the Review is of the opinion that the power to access retained data for the purpose of safeguarding the security of the State should be formally and expressly circumscribed by criteria and conditions aimed at protecting against abuse and defending the fundamental rights of individuals affected by its exercise. (**R**) Accordingly, the right of access should be limited to circumstances where there are reasonable grounds for suspecting that the person concerned poses an existing and serious threat to the security of the state. (**R**) These safeguards are intended to ensure that any disclosure is proportionate to the threat. Although essential to the operation of the rubric as a whole, the Review believes that these additional safeguards are particularly relevant to journalists – who, by virtue of the wide range of professional contacts they are required to maintain, may be especially vulnerable to disclosure requests of a more speculative or exploratory kind in the matter of state security. (**R**)

354. Finally, the somewhat Delphic reference to this rubric by the ECJ in *Tele2*is also deserving of comment. In the opinion of the Court (at paragraph 119 of the Judgment), the principle of necessity requires that disclosure requests made in the context of combating crime must be confined "as a general rule" to persons suspected of direct, or at least indirect, involvement in serious crime: i.e., ''*individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime*.'' However, the Court acknowledged that there may be "particular situations" where that general rule may not apply; adding that "*where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities*."

355. Although access to retained communications data should in general be limited to persons directly implicated and suspected of involvement in criminal activity or other unlawful activity which poses an identifiable and real threat to the security of the State, the ECJ appears to acknowledge, at paragraph 119 of its Judgment in *Tele2,*that the retained communications data of persons not themselves suspected of any such unlawful activity may, by way of exception, be accessed in accordance with the objective criteria outlined in that paragraph. These objective criteria are important in order to prevent a journalist's (or any other person's) fundamental rights being interfered with on a purely speculative basis or simply because they were identified as what is sometimes known as "a person of interest". Any application for authorisation to access the retained communications data of individuals not themselves suspected of wrongdoing should set out the basis on which that application is made, having regard to the criteria referred to above. (**R**)

Recommendations on Safeguarding Security of the State

356. It should be a requirement of legislation (whether primary or secondary) that members of the Garda Síochána and the Defence Force should, as part of the process of

submitting a proposal to a designated officer that a disclosure request be made in relation to safeguarding the security of the State, set out:

- Precise details of the serious threat to the security of the State;
- The relevance to the safeguarding of the security of the State of the data requested;
- The objective to be achieved by obtaining disclosure of the data and how this objective is to be realised;
- The attempts made to attain the objective of safeguarding the security of the State by less intrusive means,
- Where an application for access relates to a person not himself a suspect that fact should be stated and the grounds upon which the access is considered justified. (**R**)

357. It should be a formal requirement of the legislation that a designated officer should have reasonable grounds to believe that the disclosure of retained communications data is

(a) the least intrusive means available, having regard to its objectives and other relevant considerations,

(b) proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and

(c) of an extent that is reasonably required to achieve its objectives. (**R**)

Revenue Commissioners

358. The purposes for which an officer of the Revenue Commissioners may seek disclosure of retained data under section 6(3) of the 2011 Act are in substance the same as those applying to the Garda Síochána under section 6(1)(a). Section 6(3) permits an officer of the Revenue Commissioners to make a disclosure request where the officer is satisfied that the data are required for the prevention, detection, investigation or prosecution of a

revenue offence. Section 1 of the Act defines "revenue offence" as meaning any offence under specified statutory provisions "that is a serious offence". The specified statutory provisions are:

- section 186 of the Customs Consolidation Act, 1876;
- section 1078 of the Taxes Consolidation Act, 1997;
- section 102 of the Finance Act, 1999;
- section 119 of the Finance Act, 2001;
- section 79 (inserted by section 62 of the Finance Act, 2005 of the Finance Act, 2003;
- section 78 of the Finance Act, 2005.

359. That definition is subject to the general definition of "serious offence", also set out in section 1, as meaning an offence punishable by imprisonment for a term of five years or more. (Certain other offences as set out in Schedule 1 of the 2011 Act are deemed to be serious offences but these are not offences which come within the purview of the Revenue Commissioners as such.)

360. The Review has learned that the Revenue Commissioners do not normally make disclosure requests in connection with revenue offences arising under the Tax Code; the Commissioners already have at their disposal a wide range of extensive powers for the prevention, detection, investigation or prosecution of offences in this area, whether committed by individuals or corporations. However, the Revenue Commissioners are also the statutory authority with responsibility for enforcing the Customs and Excise Code and related matters and thus with the prevention, detection and investigation or prosecution of offences arising in that context. Broadly speaking, the latter include offences dealing with illicit imports, including drugs, fraud, and a host of criminal activities relating to the evasion of import taxes or duties, or of taxes and duties on particular products such as tobacco, alcohol and fuel oils. In the result, the Customs and Excise branch of the Revenue Commissioners often work in tandem with the Garda Síochána, particularly when dealing

with offences involving the importation of illicit drugs; and it is in this context that disclosure requests pursuant to section 6(3) are most frequently made.

361. Suffice it to say for present purposes that the offences covered by the various statutory provisions set out in section 1 of the 2011 Act, and reprised in the immediately preceding paragraphs, cover a myriad of revenue and customs offences. These include offences relating to the importation of prohibited goods, including drugs, or importing goods without paying relevant taxes or duties, criminal conduct relating to the making and paying of tax returns as well as criminal conduct involving the evasion of taxes or controls on specific products such as alcohol, tobacco or diesel oil. All of the provisions listed in section 1 comprehend offences which are not "serious" within the meaning of the Act of 2011 (because the applicable penalty is less than five years' imprisonment) as well as offences which are "serious offences" in the relevant sense (because a term of imprisonment of at least five years may be imposed on conviction). All of the serious revenue offences which fulfill this criterion relate to offences where a conviction is obtained on indictment only.

362. As with the other provisions in section 6 relating to the making of disclosure requests, the power conferred on the Revenue Commissioners in this regard is broadly stated: access to retained data is permitted if the relevant officer is ''satisfied that [access]is required for the prevention, detection, investigation or prosecution of a revenue offence.'' In the opinion of the Review, the powers exercised by the Revenue Commissioners in this regard, like the analogous powers exercised by the other statutory bodies with a right of access under the 2011 Act, should be circumscribed by principles and safeguards designed to ensure that the right of access is exercised proportionately, having regard to potential or actual interference with fundamental rights of the subject of the disclosure request. (**R**)

363. The aforementioned principles and safeguards should reflect those already recommended in respect of the Garda Síochána in the exercise of their analogous powers

to make a disclosure request for the corresponding purpose of combating a serious crime. (**R**)

364. Moreover, all of the so-called overarching recommendations pertaining to disclosure requests generally, as set out earlier in the Review, should also be applied to disclosure requests by the Revenue Commissioners. (**R**) As regards the information furnished in any statutory declaration made for the purpose of securing prior authorisation to make a disclosure request, the accompanying documentation should not only specify the particular 'serious' offence relevant to the request, but should explain the basis on which the offence is one which could lead to a prosecution on indictment. (**R**) As already indicated, only a conviction on indictment for one of the specified revenue offences constitutes a serious offence for the purposes of the Act.

Recommendations on Revenue Commissioners

365. A statutory declaration supporting an application by the Revenue Commissioners for prior authorisation (by a judge or independent body) should include all the information already recommended in respect of such applications generally as well as information demonstrating that the disclosure request pertains to an offence which could lead to a prosecution on indictment. (**R**)

Garda Síochána Ombudsman Commission (GSOC)

366. It will be recalled that the Garda Síochána Ombudsman Commission (GSOC) also makes disclosure requests pursuant to section 6 of the 2011 Act, even though its power to do so is not expressly mentioned in the Act or in any amendment thereto. It will also be recalled that this Review was established in the wake of public concern following GSOC's reliance on section 6 for the purpose of accessing retained communications with a view to uncovering a journalist's sources of information.

367. GSOC relies on its interpretation of the express powers conferred upon it by section 98 of the Garda Síochána Act, 2005 as the basis for making disclosure requests pursuant to section 6 of the 2011 Act. These powers are considered below.

368. GSOC was established by Part 3 of the Garda Síochána Act, 2005. Broadly speaking, its aims and objectives include promoting public confidence in the process of addressing and resolving complaints about the conduct of members of the Garda Síochána. GSOC's statutory remit includes investigatory powers in respect of criminal offences suspected to have been committed by a member of the force, as well as the power to designate an officer specifically for the purpose of conducting an investigation pursuant to these powers and under its direction. GSOC is free to engage such officer from within the ranks of the Garda Síochána or from another police service.

369. Section 98(1) of the Garda Síochána Act, 2005 provides that a designated officer, who has been directed by the Ombudsman Commission to investigate a complaint, "has, for the purposes of the investigation all powers, immunities and privileges conferred and all the duties imposed on any member of the Garda Síochána by or under any enactment or the common law including those relating to the following matters: ..." and the subsection goes on to specify certain matters, none of which specifically refer to a power to access retained communications data.

370. Section 98(2) provides that:

> *"For the purpose of sub-section 1, an enactment conferring a power, immunity or privilege or imposing a duty on a member of the Garda Síochána in relation to any other matters* specified in that sub-section *applies with the following modification and any other necessary modifications:*
>
> …

(c) A reference in the enactment to a member of the Garda Síochána not below the rank of inspector is to be read as a reference to a member of the Ombudsman Commission."

371. GSOC's interpretation to the contrary notwithstanding, it is not self-evident that the terms of section 98(2)(c) necessarily comprehend the powers reserved to an officer of the Garda Síochána not below the rank of superintendent which is the designation in section 6 of the 2011 Act. Moreover, some of the powers conferred by the 2011 Act - such as ''the safeguarding of the security of the state'' or ''the saving of human life'' - have nothing to do with GSOC's functions as set out in the 2005 Act.

372. Be that as it may, there is an evident need for greater clarity and certainty in the matter of GSOC's entitlement to make disclosure requests pursuant to section 6 of the 2011 Act. As already indicated, given the highly intrusive nature of a system of data retention and disclosure, and the concomitant threats it poses to the fundamental rights of those affected by its operation, it is essential that all avenues of access to private data should be expressly provided for within the framework of the governing enactment in the area. In short, the governing enactment should comply with the legality or clear statement principle, while legislative scatter in the matter of access should be avoided at all costs. Plainly the provisions of the principal enactment should specify the bodies entitled to issue disclosure requests; and the list of bodies thus specified should be exhaustive. (**R**) Equally plainly, disclosure requests by recognised bodies, including GSOC, should be circumscribed by verifiably objective criteria designed to ensure conformity with the principles of necessity and proportionality as elaborated in the jurisprudence of the European Court of Justice dealing with this matter. (**R**) These should include an express requirement that access by GSOC to retained data is only permitted in respect of a serious criminal offence as defined by reference to objective criteria, and excludes access to a journalist's data, or that of any other person, where the criminal investigation concerns the commission of an offence by another person. (**R**)

373. Accordingly, the overarching principles, policies and procedures that have already been recommended as regards the right of access to retained data by statutory bodies and individuals generally should be applied, *mutatis mutandis*, to GSOC. (**R**) Similarly, the obligation to obtain prior authorisation from a judge or independent body before making a disclosure request should also be applied to GSOC; although the current chairman of GSOC is a High Court judge, the concept of prior authorisation necessitates an assessment by a person or authority independent of the statutory body concerned. (**R**) Moreover, the application for prior authorisation should include information disclosing reasonable grounds for believing that the offence on which the application is based is a serious offence for the purposes of the criteria of the 2011 Act. (**R**) Finally, it goes without saying that all of the previously tabulated recommendations pertaining to the security, confidentiality and timely destruction of personal communications data should be applied with equal force to GSOC. (**R**)

Competition and Consumer Protection Commission

374. The Commission was established by the Competition and Consumer Protection Act, 2014. The extensive functions conferred on it by the 2014 Act include powers relating to the prevention, detection, investigation and prosecution of competition offences referred to in that Act and the Competition Act, 2002.

375. By virtue of section 6(3A) of the Communications (Retention of Data) Act 2011, as inserted by section 89(b)(i) of the Competition and Consumer Protection Act, 2014, a member of that Commission may request a Service Provider to disclose data retained by the Service Provider where such member is satisfied that the data are required for the prevention, detection, investigation or prosecution of a competition offence. Section 1 of the 2011 Act was similarly amended so as to define "competition offence" as meaning an offence under section 6 of the Competition Act, 2002, "that is an offence involving a agreement, decision or concerted practice to which sub-section (2) of that section applies."

376. A satisfactory aspect of these provisions is that they comply with the clear statement principle and anti-scatter policy repeatedly referred to by this Review when analysing the legislative framework governing the retention and disclosure of private communications data. The power to issue a disclosure request was conferred on the Commission by introducing an express amendment to the principal enactment, the 2011 Act, where it is easily accessible and properly contextualised – rather than by including a provision to that effect among the myriad powers and functions set out in the Competition and Consumer Protection Act, 2014.

377. Although the power to make disclosure requests has not thus far been exercised by the Commission, the Review is satisfied that, like the companion powers enjoyed by other statutory bodies recognised by the 2011 Act, it should be adjusted to ensure that it can only be exercised in accordance with the principle of proportionality and that it is accompanied by appropriate safeguards for the protection of individual rights. (**R**) In the opinion of the Review, these adjustments are particularly appropriate given the type of offence with which the Commission is principally concerned. In the nature of things, competition offences often involve clandestine activity within and between corporate entities, and are often facilitated by extensive telephony and internet communication, all of which is likely to lead to reliance on disclosure requests as an aid to investigation in the future.

378. The composition and membership of the Commission is governed by section 12 of the 2014 Act. Section 12 provides for a minimum of three full-time members of the Commission, consisting of the Chairman and two other full-time members. However, the Commission may consist of up to six full-time members in addition to the Chairman, the actual number to be determined by the Minister. Further, there may be an unspecified number of part-time members of the Commission, which number also falls to be determined by the Minister.

379. Currently there are four members of the Commission including the Chairman. Given its statutory structure, and the potential membership numbers involved, the Review

is of the opinion that the Commission should be expressly required to establish a dedicated unit for the preparation of disclosure requests and that the power to apply for prior authorisation to issue such requests should be assigned to a designated commissioner, with suitable provision being made for an alternative in the case of inability to act. (**R**) Moreover, the function assigned to the designated commissioner in this regard should be excluded from the powers capable of being delegated under section 10(6) of the 2014 Act.(**R**)

380. As in the case of other statutory bodies entitled to make disclosure requests, the Commission should firstly be subject to all of the overarching provisions recommended for the purpose of ensuring that the power of access is exercised in accordance with the principles of necessity and proportionality and is accompanied by appropriate safeguards for the protection of individual rights. (**R**) Secondly, the Commission should be subject to the recommendations already made in connection with the security, confidentiality and timely destruction of accessed data. (**R**)

381. In line with the principle of proportionality, it follows that the Commission's right of access to retained data for the purpose of combating crime should be confined to serious competition offences. (**R**) As matters stand, the 2011 Act, as amended, contains no restriction in this regard. As already indicated, section 6(3A) of the Act simply vests the power of access in the Commission in respect of ''competition offences'', while the Interpretation section defines a competition offence as an offence under section 6 of the Competition Act 2002 to which subsection 2 of that section applies. In the result, the Commission's right of access applies to a host of minor or summary offences punishable by fines of E3000 in the case of corporate undertakings, or a maximum term of 6 months' imprisonment with or without a fine, in the case of an individual. Given that section 1 of the 2011 Act defines a serious offence as an offence punishable by a term of 5 years' imprisonment or more, these offences plainly do not qualify as serious offences in the relevant sense. Nor, of course, do they meet the "serious offence" requirement of EU law as explained in *Tele2*.

382. However, the aforementioned offences may also be prosecuted on indictment, in which case the applicable penalty is a term of imprisonment not exceeding five years with or without a fine. This obviously meets the criterion of serious offence. Moreover, where the defendant is a corporate undertaking, a fine of E4 million or ten per cent of turnover, whichever is the greater, may be imposed on conviction. In the opinion of the Review, given that the question of imprisonment does not normally arise in competition cases against corporate undertakings as such, provision for fines of that magnitude elevates section 6 offences to the status of serious offences within the meaning of the criterion laid down in this regard by section 1 of the 2011 Act.

383. Accordingly, the power of the Commission to seek authorisation for the purpose of accessing retained communications data should be amended so as to refer to a "serious" competition offence with a corresponding amendment to the definition of serious offence in section 1 to allow for the conviction of a corporate enterprise for an offence punishable by a very substantial fine such as the sum of €4million referred to above. Alternatively, the definition of "competition offence" in section 1 could be appropriately revised. **(R)**

Recommendation on Competition and Consumer Protection Commission

384. The power of the Commission to seek authorisation for the purpose of accessing retained communications data should be amended so as to refer to a "serious" competition offence with a corresponding amendment to the definition of serious offence in section 1 to allow for the conviction of a corporate enterprise for an offence punishable by a very substantial fine such as the sum of €4million referred to above. Alternatively, the definition of "competition offence" in section 1 could be appropriately revised. (**R**)

385. In addition, as stated above, the recommendations concerning safeguards which apply to other statutory bodies should be applied to the Commission. (**R**)

Prior Independent Authorisation

386. By virtue of section 7 of the 2011 Act, Service Providers are obliged to comply with disclosure requests made pursuant to section 6 of the Act; there is no requirement for an accompanying warrant issued by a court or any other form of prior independent authorisation. As already indicated, this arrangement is no longer tenable following the decision of the European Court of Justice in *Tele2* (at paragraph 120 of the Judgment). As a result of that decision, prior independent authorisation is now required by European law before a Service Provider can accede to a disclosure request. It is also a safeguard that, as has been seen, is considered by the ECtHR as an important factor in determining the proportionality of such measures.

387. Changing the law to provide for this development raises important questions about the nature of prior independent authorisation, the kind of body best suited to carrying it out, how such a body should be structured, and what, if any, ancillary functions it might usefully be asked to fulfil.

388. It should be observed at the outset that while prior authorisation to disclose personal communications data impacts on the fundamental rights of the affected parties, it does not involve a determination amounting to the administration of justice. Rather it should be seen as analogous to issuing a search warrant which is an executive or ministerial act carried out (in most instances) by a judge. However, although prior authorisation is essentially an executive act, the Review is nevertheless of the opinion that it is best carried out by a person or persons with an understanding of the rights affected by a system of disclosure requests, as well as an appreciation of the public interests served by it.

389. One possible solution to this issue would be to treat prior authorisation as analogous to issuing a search warrant and thus to assign the function to the judges of the District Court. However, this course of action would put at risk a valuable aspect of the current system of administrative authorisation as practiced by both the statutory bodies

and the Service Providers: the operation of the single-point-of-contact principle within their respective organisations in connection with the issuing of disclosure requests. As previously explained, this approach promotes the development of in-house expertise and helps to maintain and improve standards. To say the least, it would be challenging to maintain and improve these standards in the event that prior authorisation was spread across the entire complement of District Court judges. Such expansion might also mean that permission to apply for disclosure requests would have to be extended to every divisional Garda Chief Superintendent in the country, thus further diluting the advantages accruing from the single-point-of-contact principle. Even if prior authorisation was confined to judges of the Dublin District (on the basis that that is where the relevant statutory bodies and Service Providers are located), the dilution of the single-point-of-contact principle would still be considerable.

390. In order to preserve the advantages of the single-point-of-contact principle the Review is of the opinion that the power to grant prior authorisation to issue disclosure requests should be conferred on a limited number of individuals. (**R**) This could be achieved as follows. Provision could be made for a set number of judges of the District or Circuit Courts to be nominated by the Presidents of those courts to hear applications for prior authorisation. Alternatively, a bespoke tribunal could be established for this purpose; it will be recalled that the ECJ in *Tele2* contemplated prior authorisation by ''*a court or by an independent administrative body*.'' Either of these approaches would preserve the benefits of specialist expertise and consistent standards associated with the single-point-of-contact principle. Moreover, both approaches would provide for the consistent availability of relevant personnel in and out of hours, thus reducing the need to issue disclosure requests without prior authorisation in cases of emergency. It should be noticed in this connection that the ECJ in *Tele2* waived the requirement for prior independent authorisation ''*in cases of validly established urgency*'' (at paragraph 120 of the Judgment). In the opinion of the Review, this exception should be provided for in national legislation, but should be accompanied by a requirement that the authority seeking disclosure must subsequently provide objective evidence of the need for urgent and immediate access

without prior authorisation, and must submit, as soon as possible thereafter, an application to the independent body or designated judge for retrospective authorisation. (**R**)

391. By the same token, both approaches to prior authorisation would allow for the conferral of ancillary responsibilities also likely to benefit from the concentration of expertise in the hands of a limited number of designated individuals. These additional functions might include those currently carried out by the Complaints Referee under the Interception of Postal Packets and Communications Messages (Regulation) Act 1993, as amended by section 11 of the 2011 Act.

392. Ultimate responsibility for data security and destruction is currently the province of the Data Protection Commissioner - the designated national supervisory authority in these matters by virtue of section 4(2) of the 2011 Act. While it may not be possible or desirable (within the framework of EU and national law on data protection) to divest the Data Protection Commissioner of these responsibilities, consideration should be given to assigning at least a supplementary data protection oversight role to any designated judges or tribunal established for the purpose of granting prior authorisation for disclosure requests.(**R**) The amalgamation of these functions would provide for more comprehensive oversight of the system of data disclosure, as well as bringing greater coherence to the operational integrity of the system.

393. It should be noted that a tribunal structure, as distinct from the nomination of a panel of judges, allows for greater flexibility in the allocation and review of key functions. For example, a tribunal structure would allow for the appointment of members with a wide range of relevant expertise – including specialist knowledge in the areas of human rights, communications technology, and forensic investigation; and would enable individual members to be stood down when decisions in which they were originally involved are being reviewed.

394. While consideration of the law governing surveillance and the interception of communications is beyond the scope of this Review, it is evident that a tribunal established to authorise and oversee the disclosure of retained communications data might also be assigned those functions in respect of cognate law-enforcement related incursions on personal privacy and associated fundamental rights.

395. As already indicated, an application by a statutory body for authorization to access a suspect's retained communications data is an investigatory power. It is analogous to an application to a judge of the District Court for a search warrant. In the opinion of the Review, the notion – suggested by some - that a suspect should be put on notice and given an opportunity to be heard so as to have a trial (possibly with an appeal) of such cases is objectively incompatible with the effective and legitimate conduct of criminal investigations in the public interest. The Review is satisfied that the balance is properly struck by the requirement of prior independent authorization, and by the recommendation as to subsequent notification of access to the persons affected when this would no longer prejudice an investigation or a prosecution, as well as that regarding the provision of sufficient remedies for those whose rights have been breached by any unlawful access.

Recommendations on Prior Independent Authorisation

396. Legislation should require that all requests for the disclosure of data made by designated officers of recognised statutory authorities are subject to prior independent authorisation by a judge or a statutorily independent tribunal. It is envisaged that exceptions could be provided for in law to address urgent situations, with an accompanying obligation to seek retrospective approval. (**R**)

397. Every decision as to whether disclosure should be authorized should be evaluated in accordance with the principle of proportionality, including the question of whether there are effective alternative means of investigation or action. Proportionality bears on the question of whether a disclosure request should be made in the first place, as well as on

the scope of the request, the nature of the data sought, and the timeframe covered by the request. (**R**)

398. Every application for prior authorisation in the form of a statutory declaration should contain all the essential information concerning the basic criteria and statutory purpose in respect of which the request is being made. (**R**)

399. In the case of a disclosure request for the purpose of identifying a journalist's sources, this purpose should be expressly stated without prejudice to all other details to be included in an application for authority to make a disclosure request. It is recommended that applications of this nature should only be made to a judge of the High Court. (**R**)

400. It is, of course, essential that any system of prior authorization be properly resourced, including, where required, by expert personnel. (**R**)

POSTSCRIPT

401. As has been demonstrated in the course of reviewing the provisions of the Communications (Retention of Data) Act 2011, the Review has felt bound to conclude that many of the features of the data retention scheme established by the Act are precluded by EU law. Accordingly, it is recommended that consideration be given to the extent that, if at all, statutory bodies should, as a matter of policy, continue to access retained communications data under the provisions of the 2011 Act pending the final resolution of issues pertaining to the status of the Act and/or any amending legislation conforming with EU law and obligations under the ECHR.

SUMMARY OF MAIN RECOMMENDATIONS

Confidentiality of Journalistic Sources

402. In light of the importance attached to the confidentiality of journalistic sources by the ECtHR as outlined above, consideration should be given to the inclusion in any amending legislation governing access to retained communications data of a provision expressly prohibiting access for the purpose of identifying a journalist's sources except in accordance with the circumstances and conditions laid down in that legislation. (**R**) By the same token, prior authorisation of the statutory body seeking access to a journalist's sources should be obtainable only from a judge of the High Court. (**R**) As explained in Chapter 3, the general recommendation as to prior authorisation is that, in line with the ruling of the ECJ in *Tele2*, such authorisation should otherwise be assigned to an independent judicial or administrative body.

403. Access to a journalist's retained communications data for any purpose, including for the purpose of identifying his or her sources, should in principle be permitted only when the journalist is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State.**(R)**

404. Accordingly, contrary to what is permitted under the 2011 Act it should not be permissible to access a journalist's retained data for the purpose of investigating an offence committed by someone else. This limitation should be subject only to the 'particular situations' (referred to at paragraph 119 of the Judgment in *Tele2)* where vital national interests such as public security are at stake and there is objective evidence justifying access. (**R**)

405. In addition, with regard to any statutory regime for the retention of communications data, express provision should be made by law prohibiting access by State authorities to retained data for the purpose of discovering a journalist's sources unless such access is fully justified by an overriding requirement in the public interest. (**R**)

406. A journalist whose retained data has been accessed should, as in the case of any other person similarly affected, be notified of the fact as soon as such notification would no longer be likely to prejudice any investigation or prosecution of a serious criminal offence. (**R)**

407. The general recommendation that express provision be made for remedies in the case of unlawful access to a person's retained communications data will, on that account, be available to a journalist who considers that his or her rights have been infringed by wrongful access. (**R**)

408. In addition to these particular safeguards, access to a journalist's retained communications data for any purpose will also benefit from the full range of safeguards recommended in respect of such access by State authorities generally. (**R**)

Conforming Legislation

409. By definition, conforming legislation should be consonant with the limitations as to the proper scope of a system of communications data retention and disclosure laid down by the ECJ in *Tele2*. (**R**)

410. Such a system should also include the full range of safeguards pertaining to the security of retained data, including its timely destruction, and the conditions of access to such data – as set out in detail in this Review. (**R**) In the fields of crime and national security, access to retained communications data should, as a general rule, and contrary to what is currently permitted, be limited to the communications data of persons reasonably suspected of being involved in serious crime or activities that pose an actual and serious threat to the security of the state. (**R**)

411. Assuming such amending legislation is enacted, it seems that any national statutory data retention framework would have to provide for the possible extension, from time to time, of its application to a region or a section of the public whose data should be retained under the umbrella of the parent Act according as objective evidence arose for the need

for such a course of action. To say the least, it would be unrealistic to expect such extending measures to be done by way of amending legislation, given the length of time such a process inevitably takes. Accordingly, legislation establishing a data retention system as envisaged by the ECJ in *Tele2* should include within its provisions the power to extend the application of a data retention regime from time to time in accordance with the criteria referred to by the ECJ. One means of doing this would be by Ministerial Order or Regulation. Any power to extend the application of an existing data retention regime along these lines would have to be by clearly defined objective criteria for the exercise of such a power. (**R**)

412. The detailed rules governing data security to which the ECJ alluded, together with the obligations imposed on Service Providers in this regard, should be expressly included in any legislation providing for a data retention and disclosure scheme. (**R**)

Data Security

413. Provision should be made by legislation for the introduction of substantive security measures, including standards and procedures to be observed by Service Providers so as to ensure effective protection and security of retained data against the risk of abuse and unlawful access or use of the data. The substantive security obligationswith which Service Providers are required to comply should be clearly stated in the principal enactment governing data retention and disclosure for specified statutory purposes. Service Providers should be placed under a statutory duty to destroy spent data, i.e., data which has been "accessed and preserved" but in respect of which the accessing body has given notice that the data in question are no longer needed for statutory purposes. (**R)**

414. Legislation should specify that retained data must be stored in Ireland, thus ensuring its security and that access to it is limited in accordance with the relevant criteria and safeguards laid down in Irish law. (**R**)

Independent Monitoring Authority

415. A supervisory authority, whether it be the Data Protection Commission or another independent authority, should be expressly designated as a monitoring authority in respect of security compliance by Service Providers in the matter of retained data. The authority should be given defined powers and duties, and endowed with appropriate expertise. Its duties should include periodically monitoring observance by Service Providers of their obligations regarding the security of communications data which they are obliged to retain. The authority should also be allocated the power to give directions to Service Providers concerning procedures and protocols to be observed for security purposes. (**R**)

416. Service Providers should be required to draw up a Compliance Statement describing and explaining in detail the security measures (including procedures and protocols) which they have put in place for the purpose of fulfilling all elements of their statutory obligations in respect of data security including protection against unlawful or unauthorised access. A copy of the Compliance Statement should be furnished annually to the supervising authority and any interim amendments or updating thereto should be notified to that authority as and when they are introduced. (**R)**

Statutory Cohesion

417. Any new or amending legislation establishing a system of data retention and disclosure should contain all of the relevant law on these matters. (**R**) The relevant law should be stated in clear and accessible language in line with the principles of legal certainty and foreseeability as articulated by the ECtHR. (**R**) Any new or amending Act should be drafted so as to identify all of the bodies or persons who may have a right of access, even if through a court application, to data currently retained under section 3 of the 2011 Act. (**R)**An express provision should be contained in the Act stating that only persons or bodies designated in the Act may have access to such data for the purposes and on the basis of an application of a kind specified in the Act. **(R)** Any grant of a right of

access or an amendment to these matters subsequently arising should be done only by way of express amendment to the principal Act. (**R**)

Statutory Bodies Generally

418. Existing legislation should be amended so as to provide that disclosure requests on behalf of each statutory authority may only be made by a limited set of Chief Superintendents, Colonels, Principal Officers, etc., who have been designated by the Garda Commissioner, Chairman of the Revenue Commissioners, Chief of Staff of the Defence Force, to exercise that function for the purposes of the Act. (**R)** In the cases of the Competition and Consumer Protection Commission and GSOC, the legislation already limits the power to make disclosure requests to members of the respective Commissions. This limitation should be maintained in any amended legislation, with an additional requirement that a maximum of three to six potential members of the Competition and Consumer Protection Commission may be designated for the purpose of making disclosure requests. (**R**)

419. It should be a requirement of legislation (whether primary or secondary) that investigators in all of the relevant statutory bodies should, as part of the process of submitting a proposal to a designated officer that a disclosure request be made set out:

- Details of the specific offence under investigation, including the relevant statutory provisions and penalties.
- The relevance to the investigation of the data being requested.
- The objective to be achieved by obtaining disclosure of the data and how this objective is to be realized – for example, if it is intended that the identification of numbers and subscriber details are to be followed up with personal interviews.(**R**)

420. Whether an attempt has been made to attain the objectives of the investigation by less intrusive means. (**R**)

421. It should be a requirement of legislation that investigating officers and designated officers of the statutory bodies should be instructed (such instruction to include a formal document) on how proportionality is to be assessed so as to ensure that it is seen and understood as a matter of fundamental rights and obligations and not merely as a question of efficiency. In the case of the Defence Forces, this requirement should apply both to the officers designated to apply for disclosure requests and to members who may apply to those officers for the purpose of initiating such requests. (**R**)

422. It should be a formal requirement of the legislation that a designated officer should have reasonable grounds to believe that the disclosure of retained communications data relating to the investigation of serious offences, safeguarding the security of the State or saving a human life is:

- the least intrusive means available, having regard to the objectives for which it is being sought and other relevant considerations;
- proportionate to its objectives, having regard to all the circumstances, including its likely impact on the rights of any person, and
- of an extent that is reasonably required to achieve its objectives.(**R**)

423. Legislation (primary or secondary) should specify the form of document, affidavit or statutory declaration, which would form the basis of either an application to a judge or to an independent authority, for authorization to make a disclosure request, including the essential elements of same. (**R**)

424. Each statutory body should be required by legislation to destroy data when no longer required for the purpose for which it was obtained. (**R**)

425. each statutory authority should have a statutory duty to report annually on the performance of its obligations, function and powers under the legislation analogous to the existing provisions. (**R)**

426. Legislation should require the publication of such reports or a summary thereof compiled by the Minister for Justice and Equality. (**R**)

Rights to Notification and Judicial Remedy

427. A statutory body which seeks and obtains access to retained communications data should be required to notify the person or persons affected as soon as such notification is no longer liable to jeopardise the investigation or purpose for which access was granted. (**R**)

428. Bearing in mind the coercive character of a data retention system, and the concomitant risk to fundamental rights associated with it, it is recommended that the statute establishing such a system should expressly provide for an appropriate judicial remedy and associated procedures for breaches of rights, including fundamental rights, occasioned by its operation. (**R**)

429. The foregoing recommendation may be reviewed in light of any form of equivalent judicial remedy which may be provided for when the General Data Protection Regulation comes into force in 2018. (**R**)

Punitive Sanctions

430. Conscious and reckless breaches of the rules governing data retention and disclosure should be treated as criminal offences, and the penalties attached thereto should be sufficiently severe so as to ensure that they are effective, proportionate and dissuasive. (**R**)

Saving Human Life

431. The statutory criterion for seeking disclosure of data for the purpose of saving human life should be strengthened by circumscribing it such that it can only be relied upon where there is a serious and proximate risk to the life of a person or persons. (**R**) The

expansion of the criterion to cases where there is an immediate and serious threat to the health and safety of an individual should be considered. (**R**)

Safeguarding Security of the State

432. It should be a requirement of legislation (whether primary or secondary) that members of the Garda Síochána and the Defence Force should, as part of the process of submitting a proposal to a designated officer that a disclosure request be made in relation to safeguarding the security of the State, set out:

- precise details of the serious threat to the security of the State;
- the relevance to the safeguarding of the security of the State of the data requested;
- the objective to be achieved by obtaining disclosure of the data and how this objective is to be realized, for example, if it is intended that the identification of numbers and subscriber details that have been in contact with the number in question be identified and followed up by further steps;
- the attempts made to attain the objective of safeguarding the security of the State by less intrusive means. (**R**)

433. It should be a formal requirement of the legislation that a designated officer should have reasonable grounds to believe that the disclosure of retained communications data is:

- the least intrusive means available, having regard to its objectives and other relevant considerations,
- proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and
- of an extent that is reasonably required to achieve its objectives. (**R)**

Revenue Commissioners

434. The principles and safeguards recommended in respect of the Garda Síochána in the exercise of their analogous powers to make a disclosure request for the corresponding purpose of combating a serious crime should also apply to the Revenue Commissioners. (**R)**

435. Moreover, all of the so-called overarching recommendations pertaining to disclosure requests generally, as set out earlier in the Review, should also be applied to disclosure requests by the Revenue Commissioners. As regards the information furnished in any statutory declaration made for the purpose of securing prior authorisation to make a disclosure request, the accompanying documentation should not only specify the particular 'serious' offence relevant to the request, but should explain the basis on which the offence is one which couldlead to a prosecution on indictment. As already indicated, only a conviction on indictment for one of the specified revenue offences constitutes a serious offence for the purposes of the Act. **(R)**

436. A statutory declaration supporting an application by the Revenue Commissioners for prior authorization (by a judge or independent body) should include all the information already recommended in respect of such applications generally as well as information demonstrating that the disclosure request pertains to an offence which could lead to a prosecution on indictment. (**R**)

Competition and Consumer Protection Commission

437. The power of the Commission to seek authorisation for the purpose of accessing retained communications data should be amended so as to refer to a "serious" competition offence with a corresponding amendment to the definition of serious offence in section 1 of the 2011 Act to allow for the conviction of a corporate enterprise for an offence punishable by a very substantial fine such as the sum of £4 million referred to above. Alternatively, the definition of "competition offence" in section 1 could be appropriately revised. (**R)**

Data Protection Acts 1988-2003

438. Having regard to the fact that section 8 of the Data Protection Acts 1988-2003 permits access to retained communications data in circumstances and for purposes precluded by EU law it is recommended that the section be repealed or at least disapplied as regards access to retained communications data. (**R**).

Access for Mutual International Assistance

439. The existing provisions of the Criminal Justice (Mutual Assistance) Act 2008 which provide for access, via court order, to communications data retained under the 2011 Act, should be reviewed. The aim of the review should be to ensure that any form of accessto retained data for mutual assistance purposes relates only to serious criminal offences; and is governed by the principles and safeguards which must apply to other forms of access to retained data in conformity with EU law and the recommendations of the Review. (**R)**

Prior Independent Authorisation

440. Legislation should expressly provide that recognised statutory authorities are subject to prior independent authorization by a judge or a statutorily independent tribunal. It is envisaged that exceptions could be provided for in law to address urgent situations, with provision being made for prompt application for retrospective authorisation in such cases. (**R**)

441. Every decision as to whether disclosure should be authorised should be evaluated in accordance with law, and, in particular, the principle of proportionality, including the question of whether there are effective alternative means of investigation or action. Proportionality bears on the question of whether a disclosure request should be made in the first place, as well as on the scope of the request, the nature of the data sought, and the timeframe covered by the request. (**R)**

442. Every application for prior authorization in the form of a statutory declaration should contain all the essential information concerning the basic criteria and statutory purpose in respect of which the request is being made. (**R**)

443. In the case of a disclosure request for the purpose of identifying a journalist's sources, this purpose should be expressly stated without prejudice to the other details to be included in an application to a judge of the High Court for authority to make a disclosure request.**(R**)

Concluding Recommendation

444. Consideration should be given to the extent that, if at all, statutory bodies should, as a matter of policy, continue to access retained communications data under the provisions of the 2011 Act pending the final resolution of issues pertaining to the status of the Act and/or any amending legislation conforming with EU law and obligations under the ECHR.