Tithe an Oireachtais
Houses of the Oireachtas

An Comhchoiste um Dhlí agus Ceart
Teach Laighean
Baile Átha Cliath 2

Joint Committee on Justice
Leinster House
Dublin 2

Tel: (01) 618 3899
Fax: (01) 618 4124
Email: justice@oireachtas.ie

33/JC/22

Ms Helen McEntee T.D.,
Minister for Justice,
51 St. Stephen's Green,
Dublin 2,
D02 HK52.

By e-mail to: EXMcHugh@justice.ie

Our Ref: JC4/5/U

RE: General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022

Dear Minister,

I am writing to you in relation to the General Scheme of the *Communications (Retention of Data) (Amendment) Bill 2022*. The Committee agreed to undertake PLS by requesting an oral briefing from Departmental Officials on this matter.

On Monday 27th June 2022, the Committee received a private briefing from your officials which provided an opportunity for members to clarify a number of matters as part of this process.

In the course of the engagement, the Committee raised a number of questions with the officials, including why this legislation was drafted now and was not drafted after the results of earlier court cases and rulings in this area; how often the preservation orders, which allow data to be retained for 90 days, can be renewed; and whether the Bill will ensure that an individual's rights in relation to data privacy will be protected.

In addition, the Committee undertook a stakeholder engagement on Thursday 30th June 2022 with Mr. Ronan Lupton SC, Dr. TJ McIntyre, the Data Protection Commission, the Office of the Garda Commissioner and the Department of Justice.
Opening statements and submissions are included as an Appendix to this Report.

In the course of this engagement, the following points were highlighted:

- The Committee acknowledges the need to strike a balance within the Bill of ensuring that citizen's rights to be free of State surveillance are upheld, while ensuring the Garda Síochána is equipped to carry out its duty of investigating serious criminal offences. The Committee is concerned that the rushed process of progressing this legislation will result in this balance not being achieved.

- Members noted with some concern a view from the Garda Commissioner's office that the investigation of serious criminal matters would be impeded by the measures within this Bill when enacted.

- The Committee was concerned that the Government only gave approval to draft the Bill on 31st May of this year, despite previous indications that the area was problematic at a legislative level. Such indications include the 2014 annulment of the European Data Retention Directive, the High Court appeal in 2019 which launched the current Dwyer hearings, the preliminary hearing of the Court of Justice of the European Union (CJEU) in the last year and even the final decision of the CJEU in April of this year. Notwithstanding that, the Bill only came before the Committee a fortnight before the Recess.

- The Committee is concerned that the rushed process and lack of mandatory consultation will lead to a Bill that is vulnerable to legal challenges, which will have serious consequences for future cases.

- The Committee notes with concern that recommendations from the Murray Report and recommendations arising from the previous pre-legislative scrutiny process on the General Scheme of *the Communications (Retention of Data) Bill 2017* are not reflected in this Bill.

- Concerns were raised at the exception being made to retain IP Source Data, which appears to be inconsistent with the single exception being for national security purposes. While there may well be a crime and policing justification to this provision it does not appear to be in line with the objectives previously expressed in the CJEU ruling.

- It was felt that the telecoms industry and all operational stakeholders would benefit from a transition period which would allow the legislation to be better understood prior to its enforcement. There may also be a lacuna created where providers are uncertain whether data currently stored is required to be deleted, whether it is subject to the new 90-day window or what the status is of data currently on file across the service providers.

- A question was raised as to the standing of other forms of data access under law enforcement powers e.g. a warrant under section 50 of the *Criminal Justice Act 2007,* or other provisions which may currently allow access to the data and how these stand subsequent to this legislation.

- Questions were raised about whether there were sufficient internal oversight mechanisms to protect against the powers within this Bill being abused.

As a result of these two engagements, the Committee makes the following recommendation in relation to the General Scheme:

- The Committee recommends that a Data Protection Impact Assessment should be carried out before this Bill is published.

- The Committee recommends that certain categories of citizens should be given separate rights under this Bill, for example journalists, to ensure that their sources are adequately protected.

- The Committee recommends that some operational guidance in the form of a Code of Conduct for service providers and or/ an industry working group would be welcomed, as it would assist in providing operational clarity to the new provisions.

- The Committee recommends that a wider consultation with relevant stakeholders should be undertaken in relation to this General Scheme, including representatives from telecoms companies.

- The Committee recommends that this legislation should include a sunset clause and the proposed revision of the *Communications (Retention of Data) Act 2011* later this year should include wider and more thorough engagement with stakeholders, to ensure the finalised version of this legislation will be robust and will withstand any legal challenges.

The Committee has now concluded PLS on this General Scheme and hopes that any matters raised as part of this process will be taken on board in the finalisation of the published Bill.

Finally, the Committee looks forward to further engagement and debate on this Bill in the course of its consideration and passage through both Houses.

Yours sincerely,

James Lawless TD
Cathaoirleach

30th June 2022

Cuirfear fáilte roimh chomhfhreagras i nGaeilge

Joint Committee on Justice

Opening Statement by Ronan Lupton SC[*]

---

28 June 2022

---

1. Introduction and background

1.1 Chairperson and members of the Joint Committee on Justice (the "**Joint Committee**"), I would like to thank you for the invitation to appear before you and to contribute to your current deliberations and discussions on the General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022 (the "**General Scheme**").

1.2 I am a Senior Counsel based in the Law Library, Dublin. I practise in the areas of commercial, competition, chancery, media, and regulatory law. I have taught criminal and constitutional law at professional level. I currently lecture at UCD on the Data Protection and Privacy Diploma course on a part time basis, in complement to my practice at the Bar.

1.3 I chair the Association of Licensed Telecommunications Operators – ALTO, CLG. I am an independent advisor to the ISPCC advising on Internet content and harm related issues. I have also recently been appointed to an Expert Group formed by Minister Catherine Martin TD to consider the issue of Individual Complaints under the Online Safety and Media Regulation ("**OSMR**") Bill 2022.

1.4 Prior to commencing practice at the bar. I was Head of Regulatory Affairs at Verizon in Dublin and I also held a pan-European interconnect policy role.

---

[*] B.A. (Hons) (Business Management); M.Sc. (Strategic Management); Dip. Legal Studies; Barrister-at-Law; PgDip (EU Competition Law); current study: M.A.(EU Competition Law)

1.5 I commenced my career in telecommunications in 1998, and I have been involved in policy formulation and matters related to the Internet and telecommunications markets since around 2002.

1.6 I have served on the Department of Justice Internet Advisory Board – IAB, the Internet Safety Advisory Council and later the Internet Safety Advisory Committee – ISAC, from 2006 until 2014. Those committees are reformed under the remit of the Minister for Communications and the group are now called the National Advisory Council for Online Safety – NACOS.

1.7 I have also served as a non-executive director of the Internet Service Providers Association of Ireland – ISPAI, which now operates and supervises the hotline.ie service.

1.8 I was appointed as a member of the Internet Content Governance Advisory Group – ICGAG,[1] in 2014 and I have also contributed to the work of the Law Reform Commission and the Report on Harmful Communications and Digital Safety.[2]

1.9 I have worked extensively in the area of service provider compliance the Communications (Retention of Data) Act 2011 and I have carefully followed all legal and regulatory developments in this area – giving rise to the General Scheme now under consideration.

2. Positioning

2.1 My evidence and remarks to the Joint Committee are made as an independent legal expert and can also be attributed to ALTO. The area of focus under discussion and review by the Joint Committee is relevant to my legal practice and pertinent to my role as ALTO chair.

[1] ICGAG Report: https://www.dccae.gov.ie/en-ie/communications/publications/Pages/Internet-Content-Governance-Advisory-Group-Report.aspx
[2] LRC Report: https://www.lawreform.ie/news/report-on-harmful-communications-and-digital-safety.683.html

2.2 On Sunday 26 June 2022, I send a set of Observations to the Joint Committee on Justice for its consideration. I do not intend to repeat those submissions here, instead I will **append** the Observations with this Opening Statement.

2.3 I intend to address four areas in my evidence to the Joint Committee:

(i) Backdrop to the General Scheme – *Digital Rights Ireland* – *Dwyer* – Section 6(1)(a) of the 2011 Act – New Communications (Data Retention and Disclosure) Bill;

(ii) Strategic Concerns – effecting State Agencies and service providers;

(iii) The Murray Report and *Corcoran* Decision; and

(iv) Other Concerns within the General Scheme.

3. Conclusion

3.1 Taking account of the three areas that I have made Observations on. I call on the Committee to take utmost account of current and emergent European Law and policy trends concerning Data Retention and the timing of this legislation prior to making any recommendations.

3.2 The Committee should report as widely as it can on the area of legislative reform and in particular concerning criminal justice matters connected to Data Retention.

3.3 It is quite clear to me that robust laws will act as a disincentive to bad faith actors, and properly enable An Garda Siochana and other State Agencies. However, as should be obvious, those robust laws must be compliant with the Constitution and Charter of Fundamental Rights, as interpreted through the various decisions of the Court of Justice of the European Union.

3.4 I make myself available to the Committee to clarify anything arising in this Statement.

Ronan Lupton SC

Chair of ALTO

Opening statement to Justice Committee – 30/6/22

General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022

Chairman and members,

Good morning, my name is Dan Kelleher. I am a Principal Officer in the Criminal Legislation function of the Department of Justice. Thank you for the opportunity to address you in relation to the General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022. I would like to note at the outset that my opening statement is without prejudice to the outcome of the current litigation in relation to data retention in the case of *GD v the Commissioner of an Garda Síochána and others, EU court of justice reference Case C-140/20*. The Court of Justice gave its ruling in this case on 5 April and the State's appeal of a High Court decision regarding the validity of a section of the Communications (Retention of Data) Act 2011 remains before the Supreme Court.

On 31 May, Government approved the drafting of the General Scheme of a Bill to amend the Communications (Retention of Data) Act 2011, on foot of the Court of Justice decision. The history of this case is that the High Court ruled, in January 2019, that Section 6(1)(a) of the Communications (Retention of Data) Act 2011 was inconsistent with the European E-Privacy Directive, read in light of the Charter of Fundamental Rights of the European Union. That subsection relates to the disclosure of certain categories of data (e.g. date and time of calls; duration; etc.) from telephony and internet communications, but not the content of such communications, by service providers to An Garda Síochána (and other bodies) in connection with the prevention, detection, investigation or prosecution of a serious offence.

A stay was placed on the judgment pending the State's appeal to the Supreme Court. Following the ruling of the CJEU (5/4/22) on a preliminary reference on relevant issues to the CJEU, it is anticipated that the Supreme Court will finalise the appeal in the near future.

The most immediate impacts of the recent ECJ ruling and previous CJEU rulings are:

1. The confirmation that general retention and indiscriminate retention of traffic and location data for the purposes of the prevention, detection, investigation or prosecution of a serious criminal offence can no longer be permitted;

2. The confirmation of the CJEU's jurisprudence) that general and indiscriminate retention of traffic and location data is only permitted for national security reasons, provided certain conditions are met;

3. Access provisions for traffic and location data must incorporate prior judicial scrutiny other than in certain urgent circumstances and in such circumstances there must be post review.

In these circumstances, a legal frailty has been confirmed by the recent CJEU ruling with regard to the 2011 Act. Law enforcement and national security concerns and operational risks arise from two fronts.

First of all, concerns have been raised by service providers with the Department of Justice with regard to the legal robustness of holding the data that is already retained under the existing 2011 Act, now that the CJEU has issued its latest ruling. In parallel, concerns exist from the point of view of national security and the prosecution of serious offences that a robust legal framework is in place for the retention and disclosure of communications data in a manner that supports these aims, while abiding by the constraints set down in the CJEU judgement.

Given the urgency of the matter, the Minister undertook to draft a General Scheme containing amendments to the Communications (Retention of Data) Act 2011 which would respond to the above impacts. The General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022, which was published by the Minister on 21/6/22, provides for:

- *Retention of traffic and location data and authorisation of disclosure of such data for national security purposes* - a mechanism is proposed which would require the Minister to apply to a designated Judge of the High Court for approval for the continued general and indiscriminate retention of traffic and location data for national security purposes. In the General Scheme, the term "Schedule 2" data is used but this Schedule refers to traffic and location data.

- *Preservation Orders and Production Orders* - amendments are proposed which would allow for an Garda Síochána, the Permanent Defence Forces, the Revenue Commissioners and the Competition and Consumer Protection Commission to make specific applications to the District Court for the preservation of certain categories of traffic and location data by service providers and the production of such data in certain circumstances. It will be possible for these agencies to apply for either or both types of order depending on the circumstances.

The General Scheme also confirms the existing power to require retention and provide for disclosure of general subscriber data, which does not refer to traffic and location data relating to the subscriber of a service. I have attached as an Appendix to my opening statement a description of each Head of the General Scheme. It is worth noting the following heads in particular:

Head 4 provides an obligation on service providers to retain "subscriber data" for a period of 12 months. The recent CJEU rulings do not require a change to the existing rules linked to the retention of subscriber data, which has less of an impact on privacy rights. The net change for subscriber data is that the retention obligation is confirmed as 12 months for all data within the meaning of that term. By contrast, different retention periods apply in the current Schedule 2 of the Principal Act for different categories of data - 24 months for Part 1 (telephony data), and 12 months for Part 2 (internet data).

Head 5 provides for a new legal mechanism governing retention of Schedule 2 data, in order to align the 2011 Act with CJEU judgements. The Minister for Justice must first carry out an assessment of threats to the security of the State. If the Minister deems the threat to be such as would require the retention of Schedule 2 data, she may apply to a designated judge of the High Court to authorise the retention of such data by service providers. The Minister is permitted to seek the authorisation of retention of data for a period of 12 months. Similarly, the designated judge may grant by order the Minister's application, if satisfied that it is necessary and reasonable in all the circumstances to do so.

Head 8 provides for a disclosure regime for an Garda Síochána and the Defence Forces to obtain access to Schedule 2 data, provided the disclosure has been approved by an authorising judge. Disclosure of Schedule 2 data, which has been the subject of a general and indiscriminate retention obligation under Head 5, can only take place on national security grounds, which has the consequence that such disclosure applications may only be made by an Garda Síochána and the Defence Forces.

Head 10 provides for a disclosure regime for an Garda Síochána to access "cell site location data" linked to an electronic device (such as a mobile phone) in urgent circumstances, where needed to protect the life or personal safety of a person or determine the whereabouts of a missing person. This type of data is defined separately from the types of traffic and location data set out in Schedule 2 and is typically very recent data which is needed on an emergency basis by an Garda Síochána.

Head 12 provides for a "Preservation Order", which may be obtained by an Garda Síochána, the Defence Forces, the Revenue Commissioners or the Competition and Consumer Protection Commission for defined reasons where approved by an authorised judge, including the need to respond to serious offences, national security and the saving of a human life. Such orders may relate to categories of subscriber data or Schedule 2 data as defined in subhead (10). There is no obligation to hand over data to a state agency under a preservation order. The obligation on the service provider is to simply preserve the data for a maximum period, currently listed as of 90 days. The state agency which applied for and was granted the preservation order will, however, be able to apply for the order to be renewed.

Head 13 provides for a "Production Order", which may be obtained by an Garda Síochána, the Defence Forces, the Revenue Commissioners or the Competition and Consumer Protection Commission for defined reasons where approved by an authorised judge. These reasons include response to a serious offence (as currently defined in Schedule 1 of the 2011 Act). Such orders may relate to categories of subscriber data or Schedule 2 data. The effect of a Production Order will be that a service provider must immediately take steps to produce and hand over to the relevant state agency the data described in the order made by an authorised judge. Such orders can be obtained in respect of certain persons, geographical areas or other defined criteria irrespective of whether retention of such data has been approved under Head 4 or Head 5. Data which may be obtained via a Production Order may already be the subject of a preservation requirement under Head 11. However, it will not be a condition of Head 12 that the data concerned is already the subject of a preservation order.

It is worth noting that the principle of judicial authorisation and only seeking access in individual cases where required has been incorporated into this General Scheme, in line with the Court of Justice rulings. I would take the opportunity to state again that in the view of the Minister, this legislation is urgently required due to the issues I have mentioned. The Minister has also stated her intention to bring forward wider reforms in the area of data retention later this year to ensure An Garda Síochána have a robust legal framework to fight crime in the modern era. That remains her intention

ENDS

Criminal Legislation
Department of Justice
29/6/22

Appendix: Provisions of the General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022

The draft General Scheme contains 17 Heads.

Heads 1 and 2 are standard provisions providing for the short title, commencement and a definition of the "principal act" being amended.

Head 3 provides for a number of new definitions to be added to the 2011 Act, most notably the definitions of "subscriber data" and "Schedule 2 data". The latter term draws from the existing 2011 Act and is intended to capture traffic and location data. The approach proposed in the draft Scheme is to provide only the minimum changes to the current data retention regime necessary to mitigate the impact of the recent CJEU ruling and protect it from further challenge. Given the emergency nature of the Scheme, the approach recognises the need to keep parameters of the new definitions consistent with the 2011 Act.

Head 4 provides an obligation on service providers to retain "subscriber data" for a period of 12 months. In this General Scheme, it is necessary to segregate the procedures governing retention of and disclosure of "subscriber data" from the same procedures governing "Schedule 2 data" (which includes traffic and location data). The recent CJEU rulings do not require a change to the existing rules linked to the retention of subscriber data, which has less of an impact on privacy rights. The net change for subscriber data is that the retention obligation is confirmed as 12 months for all data within the meaning of that term. By contrast, different retention periods apply in the current Schedule 2 of the Principal Act for different categories of data - 24 months for Part 1 (telephony data), and 12 months for Part 2 (internet data).

Head 6 is intended to replicate, as far as subscriber data is concerned, the existing powers already assigned to an Garda Síochána, the Defence Forces, the Revenue Commissioners and the Competition and Consumer Protection Commission under section 6 of the Principal Act to access subscriber data retained by service providers. The judgements of the European Court of Justice on data retention issues do not require a change to the procedures for retention and disclosure of subscriber data.

Head 7 provides for the designation of "authorising judges" from the District Court, who will have the role of deciding on applications from an Garda Síochána and the Defence Forces for disclosure of Schedule 2 data on security grounds under the arrangements set out in Head 8 below. Applications for Preservation and Production Orders, outlined in Heads 12 and 13 below, will also require the approval of an authorised judge.

Head 8 provides for a disclosure regime for an Garda Síochána and the Defence Forces to obtain access to Schedule 2 data, provided the disclosure has been approved by an authorising judge. Disclosure of Schedule 2 data, which has been the subject of a general and indiscriminate retention obligation under Head 5, can only take place on national security grounds, which has the consequence that such disclosure applications may only be made by an Garda Síochána and the Defence Forces.

Head 9 sets out a disclosure regime for an Garda Síochána and the Defence Forces to obtain access on an urgency basis to retained Schedule 2 data on national security grounds. The regime is based on approval of a disclosure application by an appropriate senior officer in both organisations.

Head 10 provides for a disclosure regime for an Garda Síochána to access "cell site location data" linked to an electronic device (such as a mobile phone) in urgent circumstances, where needed to protect the life or personal safety of a person or determine the whereabouts of a missing person. This type of data is defined separately from the types of traffic and location data set out in Schedule 2 and is typically very recent data which is needed on an emergency basis by an Garda Síochána.

Head 11 provides for a single legal obligation on service providers to comply with the requirements to disclose data as set out in Heads 8, 9 and 10.

Head 12 provides for a "Preservation Order", which may be obtained by an Garda Síochána, the Defence Forces, the Revenue Commissioners or the Competition and Consumer Protection Commission for defined reasons where approved by an authorised judge, including the need to respond to serious offences, national security and the saving of a human life. Such orders may relate to categories of subscriber data or Schedule 2 data as defined in subhead (10). There is no obligation to hand over data to a state agency under a preservation order. The obligation on the service provider is to simply preserve the data for a maximum period, currently listed as of 90 days. The state agency which applied for and was granted the preservation order will, however, be able to apply for the order to be renewed.

Head 13 provides for a "Production Order", which may be obtained by an Garda Síochána, the Defence Forces, the Revenue Commissioners or the Competition and Consumer Protection Commission for defined reasons where approved by an authorised judge. These reasons include response to a serious offence (as currently defined in Schedule 1 of the 2011 Act). Such orders may relate to categories of subscriber data or Schedule 2 data as defined in subhead (10) ("relevant data"). The effect of a Production Order will be that a service provider must immediately take steps to produce and hand over to the relevant state agency the data described in the order made by an authorised judge. Such orders can be obtained in respect of certain persons, geographical areas or other defined criteria irrespective of whether retention of such data has been approved under Head 4 or Head 5. Data which may be obtained via a Production Order may already be the subject of a preservation requirement under Head 11. However, it will not be a condition of Head 12 that the data concerned is already the subject of a preservation order.

Heads 14 and 15 complement Heads 12 and 13 by providing for the issue of Preservation Orders and Production Orders on an urgency basis by approval of a senior officer in each of the 4 state agencies listed. Such orders will have a maximum period of validity of 72 hours.

Head 16 provides for an offence provision which will apply to all of the legal obligations for disclosure, preservation or production of data under Heads 4, 5, 6, 11, 12, 13, 14 and 15. Penalties on summary conviction and conviction on indictment are listed. The Minister notes that this Head allows for a defence for a person against whom proceedings are brought that the person took all reasonable steps and exercised all due diligence to avoid the commission of the offence. The Minister considers this to be appropriate given the range of different technology systems for the management of data that are used by different service providers.

Head 17 contains a standard regulation making power for such matters which may be prescribed under the Bill. At present, only two areas which may require secondary legislation are mentioned in the General Scheme in head 8 (format of affidavits) and Head 9 (record keeping). Further areas requiring secondary legislation are expected to be identified as part of the drafting process for the Bill.

Joint Committee on Justice
Pre-legislative scrutiny of the general scheme of the Communications (Retention of Data) (Amendment) Bill 2022
Opening Statement of the Data Protection Commission
30 June 2022

Good morning, Chair and members of the Committee. My name is Dale Sunderland, Deputy Commissioner at the Data Protection Commission (DPC). I am joined by Assistant Commissioner, Gary Russell. The DPC is pleased to assist the committee today in its pre-legislative scrutiny of the General Scheme of the Communications (Retention of Data) Amendment Bill 2022.

The timing of our contribution today is somewhat unusual given the General Scheme was published just 8 days ago and the formal invite to appear before the committee issued only yesterday. The timescales involved pose challenges for the DPC in terms of both our role in assisting this committee in pre-legislative scrutiny but also in terms of our role in being mandatorily consulted by the Minister for Justice under Section 84(12) of the Data Protection Act 2018 on any proposal for a legislative measure that relates to the processing of personal data.

On foot of the CJEU judgement in April, the DPC was informed by the Department of Justice in June that a General Scheme was in preparation as an interim amendment to the 2011 Data Retention Act ("the 2011 Act"), pending fuller scale reform. The Department indicated that the DPC would be consulted and, in fact, the DPC received the General Scheme only 8 days ago. The DPC has not yet returned its observations to the Department on the General Scheme as it was advised last week by the Department that significant data-protection relevant updates to the Scheme were being made which would be reflected in a new Bill. The DPC has only received a copy of that updated Bill in the last 24 hours and will now work to prepare its detailed observations for the Department of Justice.

In the meantime, the DPC is happy to share its preliminary observations on the published General Scheme with this Committee, while acknowledging that some of what we comment on may have been addressed in an updated version of the proposed legislation. The DPC's remit relates to data-protection related rights and freedoms of individuals and our observations on the proposed Bill reflect the binding requirements in this regard set out by the CJEU.

Firstly, it is worth observing that under the current 2011 Act, the main oversight and monitoring functions are reserved for the "designated judge" as set out in Section 12 of

that Act, namely to ascertain whether the agencies prescribed to make disclosure requests are complying with the Act. However, section 11 (1A) of the Act provides that these judicial supervisory powers do not affect the functions of the Data Protection Commission. In addition, Section 4(2) of the 2011 Act - Data Security- assigns a specific role to the DPC where it is designated as the national supervisory authority. With these provisions in mind, the DPC carried out a series of audits to examine both the data security measures and the procedures and systems for processing disclosure requests by prescribed agencies. In addition, the DPC audited all Communication Service Providers (CSPs) processing such disclosure requests. General findings and recommendations arising from these audits are outlined in the DPC Annual Reports of 2016 and 2017.

In terms of the General Scheme, it clearly sets out to address the CJEU finding that mass and indiscriminate retention of electronic location and traffic data is not permitted for the purposes of combatting serious crime. In making this finding, the CJEU did however set out a number of more permissible targeted retention measures that could be deployed - subject to specific safeguards and limitations - by Member States for the purposes of fighting serious crime. In that respect, Head 5 provides for, subject to judicial authorisation and a transparency requirement to publish any order, retention of Schedule 2 data, where an existing or foreseeable national security issue is in play. It is the DPC's preliminary view that the arbitrary period of twelve months for retention is at odds with the CJEU's requirement for an assessment in each case of the period of time for which retention is actually necessary. The CJEU has made it clear that derogations to the prohibition of storage of traffic and location data may only be granted for a period of time that is strictly necessary to achieve the objective pursued.

The DPC notes the provisions that would allow by-passing of the advance judicial authorisation in the context of requiring disclosure of such Schedule 2 data, as set out under Head 9. However, it is not clear how such purportedly urgent exceptions would in the event be justified. Likewise, the means by which it will be clear a national security issue exists or is foreseen is not clear from the General Scheme. Further detail in this regard would assist the DPC's assessment of the measures.

Heads 12 – 15 give rise to concerns given the Court has said that the limited and targeted retention it sees as permissible for serious crime investigation must not be turned into mass and indiscriminate retention. In this regard, in respect of the specified bodies, themselves quite broad in range, which may access preservation or production orders for Schedule 2 data, the means by which objective targeting and limiting criteria will be established are not clear. In respect of justified urgent cases in Heads 14 and 15, the apparent lack of judicial oversight after the event is also of concern.

In light of the high risks to the rights and freedoms of data subjects inherent in the processing envisaged in the General Scheme, the DPC is of the view that the Department should have and should conduct a Data Protection Impact Assessment in relation to the processing and provisions proposed.

The DPC also notes that there is no provision in the General Scheme for the restriction of data subject rights. Such rights include access, rectification and erasure, and if restrictions are intended, we recommend these should be provided for in the Bill with a justification for why the restrictions are necessary and in what circumstances.

I hope these comments will be of assistance to the committee and I am very happy to answer the questions members may have.

Opening Statement

Communications [Retention of Data] Amendment Bill 2022

Introductions

Good morning members of the Committee. I will shortly provide an overview of An Garda Síochána's position on the **Communications (Retention of Data) (Amendment) Bill 2022,** which is focused on addressing the immediate impact of recent judgements from the Court of Justice of the European Union (CJEU) including the Graham Dwyer case.

As you are aware, in the Graham Dwyer case the Court of Justice of the European Union (CJEU) ruled that EU law prohibited the general and indiscriminate retention of electronic and location data and found that in Ireland's case, section 6(1)(a) of the **Communications (Retention of Data) Act 2011 was inconsistent with EU law**.

Members of the Committee, An Garda Siochana welcomes the **Communications (Retention of Data) (Amendment) Bill 2022.**

With regard to this Bill, we welcome the provision contained in same to seek and retain electronic traffic and location data in order to mitigate against risks posed to our National Security.

An Garda Siochana also welcomes the provisions in the Bill to allow for the lawful access to subscriber data and information on Internet Protocol (IP) addresses which will be invaluable in sensitive criminal investigations.

AGS similarly acknowledges the provision in the Bill to access location information in high risk missing person's cases to allow us to meet our **Article 2** obligations to preserve life.

AGS welcomes the fact that judicial authorisations will be required to preserve and access data and this in turn will provide reassurance to the public of the independence of the process, bolstering the protections to the right to privacy and the right to protection of personal data.

Unfortunately, from the perspective of investigating serious crime, significant difficulties are foreseen, we are however cognisant that the Bill has to conform to the jurisprudence of the CJEU. Going forward the issue of targeted retention is a challenge for all countries in the EU and not just Ireland and it is

acknowledged that the current Bill will be followed by additional legislation, intended to address other outstanding issues.

As you will probably aware, a significant feature of criminal investigations is the use of electronic traffic and location data to provide investigative opportunities to gather evidence. In that regard, there is also a positive obligation on foot of rulings by the Superior Courts in Ireland, which mandates AGS to seek out and preserve all evidence, which tends to show the guilt or innocence of a person suspected of involvement in a crime.

Under the scheme of the Bill, whilst AGS will be able to utilise Preservation and Production Orders to secure evidence, this process will be forward-looking and not retrospective. This will cause significant difficulties in criminal investigations, which usually commence post incident. However, this restriction does not arise in relation to matters relating to National Security matters.

Where the Bill will be of most benefit is where AGS is aware in advance of the communications methods being utilised by for example an Organised Crime Group, but unfortunately this is rarely the case. In the norm, many of our criminal investigations look back into the past and utilise post incident analysis. This will no longer be possible and this will be a significant challenge for criminal investigations.

AGS would urge wider consultation with Communication Service Providers during the transition phase and post the enactment of the Bill to examine the availability of data during this phase.

If any member of the Committee have any questions both my colleague and I are keen to assist.

Thank You.

Digital Rights Ireland

Opening Statement to Joint Committee on Justice

General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022

30 June 2022

Cathaoirleach and members of the Committee

I am very grateful to the Committee for the opportunity to discuss the General Scheme of the Bill with you, and particularly the extraordinary haste with which it has been put forward.

The old Yiddish definition of chutzpah is the man who kills both his parents and then seeks the mercy of the court on the grounds that he is an orphan.

I am reminded of that definition when I hear the Department of Justice assert that this Bill is urgent and therefore must evade normal democratic scrutiny.

On 21 December 2016 the European Court of Justice gave its decision in the *Tele2*[1] case. After that date, every competent lawyer knew that Irish rules on data retention were in breach of European law. In case there was any doubt, in April 2017 the former Chief Justice, John Murray, delivered a report finding that the Communications (Retention of Data) Act 2011 amounted to illegal mass surveillance of every person in the State.[2]

But for five years since, successive Ministers for Justice have done almost nothing to remedy this breach.

They certainly did not do the responsible thing, which would have been to stop the use of the powers under the 2011 Act and arrange for it to be repealed and replaced by legislation which complies with fundamental rights. Instead they persisted in the use of a clearly illegal power, corroding the rule of law and storing up trouble for later prosecutions which have been undermined as a result.

The Department of Justice did publish a Heads of Bill in 2017.[3] However that was not a good faith response to either the judgment in *Tele2* or the Murray report. At the time Digital Rights

[1] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige/Watson* EU:C:2016:970.

[2] John Murray, 'Review of the Law on the Retention of and Access to Communications Data' (Dublin: Department of Justice and Equality, April 2017), http://www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf.

[3] Department of Justice and Equality, 'General Scheme of the Communications (Retention of Data) Bill 2017', 3 October 2017, http://www.justice.ie/en/JELR/General_Scheme_-

Ireland submitted – and the predecessor to this Committee accepted in its pre-legislative scrutiny report[4] – that the 2017 Heads of Bill failed to meet the standards of EU law in multiple regards, from the lack of protection for journalists' sources, to the failure to provide adequate oversight of the system, to the lack of an adequate judicial remedy against abuse.

Incredibly, essentially all of those points remain true of the current Heads of Bill: in particular, there is still no protection for journalists' sources, nor an adequate oversight system, nor an adequate judicial remedy for abuse. It appears to me to show fundamental disrespect to the work of pre-legislative scrutiny to ignore these findings of the Committee.

I will elaborate on these points further during the discussion but regret that I have not had the time to produce a full submission – these Heads of Bill have been rushed out without any prior consultation with industry or civil society, in an attempt to sandbag any opposition through manufactured urgency. Also, I have no reason to believe that the Data Protection Commission was notified or given a draft. This is itself in breach of the GDPR and Data Protection Act 2018, which require prior consultation before measures of this sort, and shows further disrespect to the process which the law requires for input into legislation.[5]

The Minister for Justice is, in effect, saying "trust us" to the Houses of the Oireachtas. Trust us to bypass normal democratic scrutiny. Trust us to do away with pre-legislative scrutiny and the input of the Data Protection Commission. Trust us to legislate at haste for mass surveillance of the entire population. But in the case of data retention, trust has clearly been forfeited.

Dr. TJ McIntyre

Communications(Retention_of_Data)_Bill.pdf/Files/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf.

[4] Joint Committee on Justice and Equality, 'Report on Pre-Legislative Scrutiny of the Communications (Retention of Data) Bill 2017' (Houses of the Oireachtas, January 2018), 32/JAE/22, http://www.oireachtas.ie/parliament/media/committees/justice/2018/Data-Retention-Report-Final.pdf.

[5] Section 84(12) Data Protection Act 2018; see also Article 36(4) GDPR.

To: **The Justice Committee**

Re: **General Scheme – Communications (Retention of Data) (Amendment) Bill 2022**

OBSERVATIONS

1. BACKGROUND

1.1 Ireland has traditionally required telecommunications companies to log or retain metadata or raw telecommunications data, either by Ministerial Order,[1] or by operation of law.[2] Data retention has been a required feature of State security considering the history of troubles in Northern Ireland and the emergence of serious crime and gangland activity in the State.

1.2 The European Union ("**EU**") passed two data retention Directives with relative haste, in 2002 and 2006, the backdrop to both Directives being terrorist activity in the US – 9/11 attacks, and in Europe – London and Madrid bombings. Ireland and some other EU Member States had challenged the status and passing of the 2006 Directive at that time – yet the 2006 Directive endured until 2014.

1.3 On 26 January 2011, the Houses of the Oireachtas passed an Act entitled the Communications (Retention of Data) Act, 2011 ("**the 2011 Act**"). The 2011 Act was an Act *to give effect to* the 2006 Directive or, Directive 2006/24/EC, more commonly known as the Data Retention Enforcement Directive ("**DRED**").

1.4 The 2011 Act mandated service providers to retain raw telephone records (without content) for a period of 2-years, and IP metadata for a period of 1-year, from the date of the making or origin of the relevant communication. Retention is covered by section 3 of the 2011 Act.

1.5 Disclosure could be sought by a member of An Garda Siochana not below the rank of Chief Superintendent; an Officer in the Permanent Defence Forces; and a Principal

[1] Section 98 of the Postal and Telecommunication Services Act 1983 (Ministerial Order).

[2] Section 63 of the Criminal Justice (Terrorist Offences) Act 2005.

Officer of the Revenue Commissioners. Disclosure is covered by section 6 of the 2011 Act and currently operates in the absence of any proper independent oversight.[3]

1.6 Disclosure could be required in certain circumstances, set out at section 6(1) of the 2011 Act. Namely:

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

(b) the safeguarding of the security of the State; and

(c) the saving of human life.

1.7 The 2011 Act was not without its difficulties. In particular, the State did not provide any particular regulations or direction as to how the various aspects of the 2011 Act would work in practice. This posed serious practical difficulties for the service providers and the State agencies listed as to how those parties could practically make the newly permitted disclosure requests.

1.8 The State agencies and service providers drew-up a Memorandum of Understanding ("**MOU**") setting out fairly simple terms and compliance points in order to make the 2011 Act work as practically and as feasibly as it could between the service providers and the State agencies required to operate under it. Simple matters like points of contact, points of escalation, and formats (or *Golden Copies*) of data to be disclosed were drawn up and discussed. While it is not the function of legislation to provide a detailed and prescriptive set of measures, certainly the dearth of guidance was a huge problem for stakeholders from the inception of the 2011 Act.

1.9 On 8 April 2014, the Court of Justice of the European Union ("**CJEU**") annulled the DRED in a case taken by the Irish rights group, *Digital Rights Ireland* ("**DRI**"). The Irish High Court having referred certain questions of European Law to the CJEU for clarification in or around 5 May 2010.

1.10 The effect of the annulment of the DRED in 2014, was to render the procedures of wholesale, mass and indiscriminate recording and storage of metadata or raw telecommunications data unlawful on a pan-European basis (a CJEU annulment operates as though the law had never existed in the first place). This posed a huge issue

[3] The designated High Court judge does not review disclosure requests on an *ex-ante* basis, but rather reviews the operation of the 2011 Act, on an *ex-post* basis and in isolation.

for the 2011 Act and for the State, yet no steps were taken to update the law,[4] despite various *other cases* and challenges being sent to the CJEU between 2014 and 2022 concerning data retention.

1.11 Those other cases and challenges brought to the CJEU refined the position down,[5] such that the CJEU was able to indicate relatively clearly what the proper position is concerning retention of data and for what purposes it can be said to be lawful.

1.12 A now famous and ultimately successful challenge was mounted by convicted murderer Graham Dwyer in 2015 against the 2011 Act. The annulment in 2014 of the DRED in the *Digital Rights Ireland* case provided an adequate backdrop by which to challenge the data retained by An Garda Siochana and later used, in-part, to secure a murder conviction against Graham Dwyer.

1.13 On 6 December 2018, Mr Justice Tony O'Connor handed down a lengthy judgment in the *Dwyer* challenge dealing with sections 3 and 6 of the 2011 Act.[6] Finding that both sections were repugnant to the Constitution.

1.14 However, on 11 January 2019, the Court revised the position in a second *Dwyer* judgment, or as it said itself, it "*tailored*" its declaration to deal only with the position of disclosure under section 6(1)(a) of the 2011 Act,[7] which reads:

> *"6.— (1) A member of the Garda Síochána not below the rank of chief superintendent 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—*
>
> (a) *the prevention, detection, investigation or prosecution of a serious offence*"

1.15 What ended-up being appealed to the Supreme Court in *Dwyer* was in-effect only section 6(1)(a) of the 2011 Act concerning the prevention, detection, investigation or

---

[4] Pre-Legislative scrutiny had commenced on a *Communications (Retention of Data)(Amendment) Bill 2017*, but that was not reached or tabled during the currency of that Dail session or the next session as it happens.

[5] *La Quadrature du Net and Others* C-511/18 and C-512/18 EU:C:2020:791; *Ordre des barreaux francophones et germanophone and Others* C-520/18, EU:C:2020:791; *Digital Rights Ireland and Others* Cases C-293/12 and C-594/12, EU:C:2014/238; *Tele2 Sverige and Watson and Others* Cases C-203/15 and C-698/15, EU:C:2016:970; *Ministerio Fiscal* Case C-207/16, EU:C:2018:788; *Privacy International* Case C-623/17, EU:C:2020:790; *Prokuratuur* Case C-746/18, EU:C:2021:152.

[6] *Graham Dwyer v Commissioner for An Garda Siochana & Ors.* [2018] IEHC 685. High Court O'Connor J – Judgment dealing with accessing of data – 6 December 2018 – Sections 3 (Obligation to retain data) and 6 (Disclosure request) of Communications (Retention of Data) Act 2011 repugnant to the Constitution: https://www.courts.ie/acc/alfresco/37f5f57c-0173-4e22-8cd8-d608d16fbe4f/2018_IEHC_685_1.pdf/pdf#view=fitH

[7] *Graham Dwyer v Commissioner for An Garda Siochana & Ors.* [2019] IEHC 48 – 11 January 2019: https://www.courts.ie/acc/alfresco/37f5f57c-0173-4e22-8cd8-d608d16fbe4f/2018_IEHC_685_1.pdf/pdf#view=fitH

prosecution of serious offences, but not the residual aspects of the 2011 Act, which arguably also fall foul of the annulment judgment in the *Digital Rights Ireland* case as well.

1.16 On 24 February 2020, Chief Justice Frank Clarke handed down judgment on appeal in *Dwyer* and referred six questions or EU law to the CJEU in the case.[8]

1.17 On 18 November 2021, CJEU Advocate General Campos Sanchez-Bordona rendered his preliminary opinion (such AG opinions are followed by the CJEU circa 75% of the time) in *Dwyer* (now called *G.D.*) or Case C-140/20,[9] wherein the Advocate General effectively queried: "*Why is this subject matter back here again?*"

1.18 On 5 April 2022, the CJEU rendered judgment following the Advocate General's Opinion in *Dwyer* or *G.D.* Case C-140/20.

1.19 The CJEU said the following in *Dwyer*:[10]

> *"In the light of Articles 7, 8 and 11 and Article 52(1) of the Charter,* ***must be interpreted as precluding legislative measures which provide, as a preventive measure****, for the purposes of combating serious crime and for the prevention of serious threats to public security, for the general and indiscriminate retention of traffic and location data.*
>
> *However, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter,* ***does not preclude legislative measures that****, for the purposes of combating serous crime and preventing serious threats to public security, provide for:*[11]
>
> (i) *the targeted retention of traffic and location data, which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for*

[8] *Graham Dwyer v Commissioner for An Garda Siochana & Ors.* [2020] IESC 4

[9] AG Opinion in *G.D. v AGS* or Case C-140/20 https://curia.europa.eu/juris/document/document.jsf?text=&docid=249522&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1983552

[10] CJEU Judgment in *G.D. v AGS* in Case C-140/20 of 5 April 2022: https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1983552

[11] In paragraph 168 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791),

a period that is limited in time to what is strictly necessary, but which may be extended;

(ii) *the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;*

(iii) *the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and*

(iv) *Recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers.*

Provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse."

1.20 On 26 May 2022, the Supreme Court dismissed the State's appeal of the Judgments of Mr Justice O'Connor in *Dwyer* and made orders on consent concerning the repugnancy to the Constitution of section 6(1)(a) of the 2011 Act.

1.21 On 21 June 2022, and in response to the *Dwyer* ruling by the CJEU, Minister McEntee published the: *General Scheme – Communications (Retention of Data) (Amendment) Bill 2022* ("**the General Scheme**").

1.22 The General Scheme contains 17 Heads, and it has been published with the *caveat* that another larger Bill designed to deal with the issues in both the *Digital Rights Ireland* and the *Dwyer* judgments and entitled: *the Communications (Data Retention and Disclosure) Bill* is due to be resumed and drafted (to completion) in Q.3 – Q.4 2022.

2. DISCUSSION

Strategic Concerns

2.1 The service providers, or telecommunications industry, is about to be required to make not insignificant nor cheap changes to the modes of operation it has become accustomed to since the passing of the 2011 Act.

2.2 Examples of not insignificant and costly changes arise under the following Heads:

Head 4: Change to retention periods from 2 years and 1 year, to 1 year for all data.

Query: Has the State considered the position in the interregnum? That being where retained data within the 2-year period, might fall off a cliff and impact investigations that a currently in-being?

Head 5: Ministerial security threat provision – new, 1 year time limit.

Head 6: Widening of State agency access – now including the CCPC and various Coroners.

Query: There is no guidance or procedures in-being for authorisation or simple points of contact, e.g., where does CCPC, or Coroner convey obtained court order to – perhaps the making of regulations might serve to cure such a gap or requirement.

Heads 9/10/11: Disclosure in the case of urgency, 72 – hours.

Query/Issue: This is an entirely new development, and a practical issue arises around service provider weekend and holiday and emergency cover, which ordinarily would not arise – or be available – under the current regime, or 2011 Act.

Head 12: Is an entirely new development requiring preservation for 90-day periods of time.

Query/Issue: Yet again, no guidance arises or has been issued as to how data is to be preserved, so as to ensure that the chain of evidence is kept sacrosanct. Does the individual in a service provider responsible for preservation need to certify her actions, in the event that they leave the employ of the service provider, or are incapacitated at the time of trial?

Head 13: This appears to be almost identical to the mode of operation currently in-being, with the new addition of an authorising judge permitting access on the application of the relevant State agency.

Heads 14/15 – Preservation and Production in the case of urgency: Create both 72 hour and 90-day obligations on service providers subject to threat of sanction or offence if not complied with.

Query/Issue: This is a matter of concern, given the lack of guidance and change in procedures contemplated by the General Scheme, that may be made effective or implemented in a very short timescale.

Head 16: The General Scheme contemplates offences, seven in number, that have a maximum threshold of €500,000 or 5-years in prison.

Query/Issue: This is again a matter that is news to the service providers and possibly one that might be seen as an incentive, but actually act to the contrary.

2.3 The State, via the Minister for Justice, has been in correspondence with IBEC TII and ALTO, however the timeframe between publication of the General Scheme and the proposal to pass this legislation is extraordinarily tight. That is, if the proposal remains to pass the General Scheme prior to the Oireachtas summer recess in July as a target.

2.4 Ideally, service providers should have been consulted well in advance of the drafting of the legislation to gauge what can be achieved in a tight time period. This is particularly troubling given that the General Scheme proposes seven new offences that service providers will be subject to, potentially at the time of enactment. The Minister should consider the proportionality position of that vista, and not enact the offence provisions or provisions where very significant IT developments are required (production, preservation and urgent cases) until a time period of three to six months passes, to enable service providers to quickly arrange themselves and their operations in order to comply with the law as it will shortly be.

2.5 The Minister should consider directing her officials to consider whether the making of regulations under the General Scheme could provide some guidance to the service providers concerned with the operation of the 2011 Act and new General Scheme.

2.6 It is unlikely that a sunset regime will find favour with the Minster, but the service providers affected by the changes to the General Scheme should not be subject to immediate compliance and threat of criminal sanction where emergency legislation is required to be passed, mandating significant operational changes with little or no prior notice or consultation.

The Murray Report / Corcoran Decision

2.7 On 27 April 2017, former Chief Justice John L. Murray published a report ("**the Murray Report**") entitled: "*Review of the Law on the Retention of and Access to Communications Data*".[12] The Murray Report focussed on the subject of journalists and journalist source confidence, in light of issues surrounding GSOC applications for journalists' telephone records.

2.8 The Murray Report recommended the deployment of European Union and ECHR norms in the Irish context when dealing with the position of journalists being made subject to inquiries and orders under the 2011 Act.

2.9 The question of journalistic privilege (and whether it can be said to exist at all) in Ireland, remains an issue that the Oireachtas must address, that is given the nature of the political system and future changes. Furthermore, excessive court time is being taken-up by media organisations being compelled to handover source data, that often arises in similar terms to those dealt with by the 2011 Act and the General Scheme. Such records should be protected, and disclosure requests be challengeable in court as a matter of law.

2.10 The Murray Report should not be ignored in the context of the General Scheme and also in that regard, the recent judgment of Costello J of the Court of Appeal in *Corcoran*[13] is also instructive.

2.11 The *Corcoran* judgment sets of 28 principles concerning access to a journalist's telephone, data, contacts and records and the protection of the Constitutional right to

[12] Murray Report 27 April 2017: https://www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf

[13] *Corcoran & anor v The Commissioner of An Garda Síochána & anor* [2022] IECA 98, 22 April 2022.

freedom of expression codified at Article 40.6.1.i and Article 11 of the Charter of Fundamental Rights of the European Union.

2.12 Three notable aspects of the Murray Report and *Corcoran* that should be deployed in the General Scheme and the forthcoming *Communications (Data Retention and Disclosure) Bill* are:

(a) A clear requirement and jurisdiction for authorising judges (as defined) to hold *inter-partes* hearings re. applications by State agencies for: warrants, preservation, production and disclosure orders concerning journalists (where deemed appropriate);

(b) A clear requirement for legislation to properly protect sources more generally to include in discovery; and

(c) Legislation requiring those State agencies applying to the courts (including lower courts) under the 2011 Act and General Scheme in seeking warrants preservation, production and disclosure orders concerning journalists, to be required to fully and faithfully disclose all relevant details concerning the subject or target of those applications (particularly where journalists are concerned) with a view to upholding legal rights more generally.

Other Concerns

2.13 The Section 3A procedure arising at Head 5 appears to require some more consideration. The Head as drafted appears to indicate that the proposal is an administration of justice function.

2.14 If it is an administration of justice function, then there may be a requirement for the General Scheme to permit parties effected by orders to be heard in open court. If it is not, then the State should contemplate establishing a formal independent authority with actual expertise in order to handle such matters.

2.15 Separately, and in the absence of an expert independent authority, there needs to be more consideration about how the designated judge is assigned to the task at section 3A. Presumably the President of the High Court would maintain the logical home for

such significant measures as those contemplated under the General Scheme and as a function of the administration of justice.[14]

2.16 In relation to Head 13, it appears that it may leave the door open to access for civil litigation (file sharing, defamation). The *Dwyer* decision requires that decisions to impose national security data retention be reviewable by an independent authority. Does handing the initial decision to an independent authority suffice? In that there is no *ex-post* assessment of necessity. Certainly, in the context of journalists and other parties where the General Scheme should provide jurisdiction for *inter-partes* (two sided hearings) where the interests of justice so dictate from the District Court to the High Court as the case may be, this gives rise to a concern.

2.17 It might also be appropriate to consider *ex-post* review, as has been done elsewhere in the General Scheme, in cases of extreme emergency or urgency, but relevant to the subject of production arising at Head 13.

2.18 More generally, in order to ensure compliance with the conditions to be satisfied by legislation governing access to retained data, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, within the framework of procedures for the prevention, detection or prosecution of crime.

2.19 One of the requirements for that prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access.

2.20 If the prior review is entrusted to an independent authority, that authority must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence.

[14] Usually, such tasks are purely administrative, rather than being formally an administration of justice kind of role or task. This is ventilated in the case of *Damache v DPP* [2012] IESC 11; [2012] 2 IR 2 and the *Corcoran* decision mentioned above.

2.21 Specifically, the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field, the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings.

2.22 The General Scheme needs to provide more safeguards than it currently does. It does not contemplate or permit what might be *bona fide* and required challenge, yet that is why the Murray Report and General Scheme exist at this stage.

3. CONCLUSION

3.1 It is regrettable that the State did not work to legislate more quickly when the *Digital Rights Ireland* case resulted in the annulment of the DRED and effectively made redundant aspects of the 2011 Act. It had eight years to do so.

3.2 It is arguable that aspects of the 2011 Act and the General Scheme if enacted, could still be subject to legal challenge. Whether such challenges would be successful is a matter for the courts to determine.

3.3 In the usual course, the Justice Committee should have an opportunity to draft a formal report as a result of pre-legislative scrutiny. In the event that a Justice Committee Report follows, it would be useful to remark that the State is passing the General Scheme in emergency circumstances where it has little choice but to proceed with the legislation.

3.4 The General Scheme does endeavour to faithfully meet the requirements of the various judgments of the CJEU, yet it retains a data retention regime framed under the now annulled DRED of 2006 and enabled by the 2011 Act. This means that the *Communications (Data Retention and Disclosure) Bill* must be resumed and drafted (to completion) in Q.3 – Q.4 2022, as publicly indicated by the Minister and her officials. Furthermore, the *Communications (Data Retention and Disclosure) Bill* heads should be published quickly and then consulted upon fully with all service provider stakeholders, with a view to making the transition to a new regime seamless and providing scope for input on a proper and consultative basis for the safeguarding of the

security of State, the prevention, detection, investigation of serious crime, the saving and preservation of life and the enabling of law enforcement of act in urgent circumstances without fear of obstruction.

3.5 The General Scheme is likely to proceed and be enacted without the benefit of proper consultation with the service providers who will be required to operate the new legislation at their own expense. This is not an ideal scenario.

3.6 The Committee should recommend to the Minister and her Officials that she should consider suspending the enactment of the criminal sanctions within the General Scheme on notice of the service providers, for a period time. That is due to and considering the speed at which the General Scheme has been published and is required to be passed into law without full and formal consultation.

3.7 The Committee should also recommend that the Minister and her officials use regulations and service provider contacts to ensure that what is proposed in the legislation is actually workable – whether by Code of Conduct – Memorandum of Understanding, or some other method, to enable engagement between the State Agencies and service providers, and importantly in order to meet the expectations, principles, and policies of the legislation as it is proposed to be drafted.

Dated the 26th day of June 2022

RONAN LUPTON SC

	Title: COMMUNICATIONS (RETENTION OF DATA) (AMENDMENT) BILL 2022 ARRANGEMENT OF SECTIONS	Function/Additions:	Remarks:	Other:
	PART 1 - PRELIMINART AND GENERAL			
Head 1	Short title and commencement	Name and activation only		
Head 2	Definitions	Principal Act clause		
	PART 2 - DATA RENENTION AND DISCLOSURE			
Head 3	Amendment of section 2 of the Principal Act (definitions)	"authorising judge", "communication", "disclosure requirement", "electronic communications network", "electronic communications service" "Schedule 2 data", "subscriber", "subscriber data"	**New definitions;** more granularity on subscriber data, supervision.	
Head 4	Amendment of Section 3 of the Principal Act (obligation to retain subscriber data)	Subscriber data v Schedule 2 data. The net change for subscriber data is that **the retention obligation is confirmed as 12 months for all data within the meaning of that term**.	**New Retention Period.** Contrast current: 24 months telco records and 12 months IP.	
Head 5	Insertion of new section 3A into the Principal Act (obligation to retain Schedule 2 data)	State security provisions. Timing and application provisions. Designated judge of the High Court.	**New section:** Ministerial State security threat provisions. Applies to all service providers. Temporal limitation: 12 months	
Head 6	Amendment of section 6 of the Principal Act (Requirement to disclose subscriber data)	Substitution of existing s. 6.	Widening of State agency access - CCPC and Coronors now also included.	
Head 7	Insertion of new section 6A into the Principal Act (Authorising Judges)	New preservation and production (Heads 12 and 13) order procedures via authorising judges.	**New Procedure:** District Court Judges as authorising judges	
Head 8	Insertion of new section 6B into the Principal Act (Authorisation to require disclosure of Schedule 2 data)	New section 6B inserted into Principal Act. Provides for a disclosure regime for an Garda Síochána and the Defence Forces to obtain access to Schedule 2 data, provided the disclosure has been approved by an authorising judge. (State security)	**New Procedure:** (a) made in the absence of, and without notice of the application being given to, the person to whom the data relates or the service provider who has possession of the data, (b) made on affidavit in such form as the Minister may prescribe, and (c) heard otherwise than in public	
Head 9	Insertion of new section 6C into the Principal Act (Requirement to disclose Schedule 2 data in case of urgency)	New section 6C inserted into Principal Act. Requirement to disclose Schedule 2 data in case of urgency. Note: subhead 12 - authorisation expiry in 72 hours. Requirement to reports to authorsing judge(s) within 7 days. More specific on forms of data to be specified as a 'class' of data.	**New section:** Sets out a disclosure regime for an Garda Síochána and the Defence Forces to obtain access on an urgency basis to retained Schedule 2 data on national security grounds. The regime is based on approval of a disclosure application by an appropriate senior officer in both organisations. each instance of the use of the urgent disclosure procedure must be reported within 7 days by an Garda Síochána or the Defence Forces, as appropriate, to an authorised judge.	
Head 10	Insertion of new section 6D into the Principal Act (Requirement to disclose cell site location data in case of urgency)	New section 6D inserted into Principal Act. Requirement to disclose cell site location data in case of urgency. Similar to 6C, above.	As above (6C) with limitations at sh. 12. Is intended to provide for a disclosure regime for an Garda Síochána to access cell site location data in urgent circumstances, where needed to protect the life or personal safety of a person or determine the whereabouts of a missing person.	
Head 11	Insertion of new section 6E into the Principal Act (Requirement to disclose Schedule 2 data)	New section 6E inserted into Principal Act. Requirement on operators across previous three heads 8, 9, and 10	General requiremen on operators to disclose data at Heads 8, 9, and 10.	
Head 12	Insertion of new section 7A into the Principal Act (Preservation Order for relevant data)	Insertion of a new section 7A into the Principal Act. Preservation Order procedure. Authorising judge regime - need to respond to serious offences, national security and the saving of a human life.	**New - Order to preserve - BUT not to hand over or disclose.** The obligation on the service provider is to simply preserve the data for a maximum period of 90 days. The state agency which applied for and was granted the preservation order will, however, be able to apply for the order to be renewed for maximum periods of 90 days at a time. Failure to comply is an offence.	
Head 13	Insertion of new section 7B into the Principal Act (Production Order for relevant data)	Insertion of a new section 7B into the Principal Act. Production Order procedure. These reasons include response to a serious offence (as currently defined in Schedule 1 of the 2011 Act), national security and the saving of a human life.	The effect of such an order will be that a service provider must immediately take steps to produce and hand over to the relevant state agency the data described in the order made by an authorised judge under subhead (1). **Orders can be obtained in respect of certain persons, geographical areas or other defined criteria irrespective of whether retention of such data has been approved under section 3 or 3A.** **It is not a requirement that a Preservation Order preceeds a Production Order. Appear to be separate and stand alone.	
Head 14	Insertion of new section 7C into the Principal Act (Preservation Order for relevant data in case of urgency)	Insertion of a new section 7C into the Principal Act. A temporary preservation order, in respect of relevant data if he or she is satisfied that the data is in imminent danger of destruction or otherwise being rendered unavailable.	Order issued under subsection (1) shall cease to have effect upon the expiration of 72 hours from the issue of the order. Head 12 conditions relating to preservation of the data required - assume that means 90 days but only after application and approval ro preserve on a less temporary basis.	Section numbering is now wrong in body drafting of the scheme. Says "after 7B" but publishes a 7B instread of a section 7C.
Head 15	Insertion of new section 7D into the Principal Act (Production Order for relevant data in case of urgency)	Insertion of a new section 7D into the Principal Act. Same requirements as Head 13. A temporary production order.	Order issued under subsection (1) shall cease to have effect upon the expiration of 72 hours from the issue of the order. Head 12 conditions relating to preservation of the data required - assume that means 90 days but only after application and approval ro preserve on a less temporary basis.	
Head 16	Insertion of new section 12A into the Principal Act (Offences)	New Offences by insertion of section 12A into Principal Act. (1) A person who contravenes any of the following provisions shall be guilty of an offence: (a) section 3, (b) subsection (7) of section 3A , (c) subsection (10) of section 6, (d) subsection (2) of section 6E (e) subsection (9) of section 7A (f) subsection (9) of section 7B (g) subsection (5) of section 7C (f) subsection (5) of section 7D	A person guilty of an offence under this section shall be liable – (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or (b) on conviction on indictment, to a fine not exceeding €500,000 or imprisonment for a term not exceeding 5 years or both. Where an offence under this section is **committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence**.	
Head 17	Insertion of new section 12B into the Principal Act (Regulations)	New Section 12B - Power to make regulations.	21-day period for the making of regulations.	

To: **The Justice Committee**

Re: **General Scheme – Communications (Retention of Data) (Amendment) Bill 2022**

TELCO OBSERVATIONS

1. **ADDITIONAL OBSERVATIONS**

1.1 In addition to the submission made to the Joint Committee on 26 June 2022, the following more detailed points are of significance to the telecommunications industry and service providers (as defined in the 2011 Act) concerning the General Scheme – Communications (Retention of Data) (Amendment) Bill 2022 (the "**General Scheme**"):

(a) A rough estimate of the time required to develop IT systems capable of complying with the obligations set out in the General Scheme is 12 – 24 months. Quite apart from the time and huge costs required to carry out such work, it is it is also of grave concern that the General Scheme provides at Head 16 for a number of offences in the event of a failure to comply with certain provisions, when compliance with them will not be possible for some significant time.

(b) The General Scheme does not explicitly close off routes of access to data other than via the data retention legislation itself, e.g., Section 50 of the Criminal Justice Act, 2007. Service providers would welcome an explicit provision stating that they are not obliged to comply with such warrants or with a request for data made under any means other than those set out in the legislation.

(c) Industry notes that the CJEU states in paragraph 100 of *G.D. v The Commissioner of the Garda Síochána and Others* that data retained for that purpose cannot be accessed in the context of criminal proceedings. However the General Scheme does not explicitly state whether or not data retained under Section 3A (State Security) may be accessed in order to satisfy a

Preservation Order under Section 7A. Industry would welcome the inclusion of a provision explicitly clarifying this, to ensure that both service providers and Agencies are *ad idem* in respect of the circumstances when data may be preserved and accessed.

(d) The General Scheme proposes to limit the extent of data being retained by service providers, in comparison with the 2011 Act. Industry notes however that the General Scheme does not provide for any transitional arrangements regarding the disposal of data which is held today under the 2011 Act. Industry would welcome provisions setting out the means and timelines by which service providers are obliged to delete data which is held in excess of the retention periods set out in the General Scheme. In this regard industry notes that the General Scheme would not at the date of commencement require the retention of any data, until or unless the appropriate court orders are sought and granted. Service providers are concerned that absent such orders being made, no legal basis would exist under Data Protection law for the ongoing retention of data currently retained under the 2011 Act. Industry reiterates the points made earlier in submission (and the various correspondence to the Department of Justice sent by IBEC TII) that much of the data currently retained is retained solely in order to comply with the 2011 Act and for no other purpose.

(e) In light of these concerns regarding service providers' compliance with our Data Protection obligations, industry notes that Section 84(12) of the Data Protection Acts 1988 – 2018 requires that, in the context of the processing of personal data for law enforcement purposes, where there is a proposal for a legislative measure for which a Minister of the Government is responsible that relates to the processing of personal data, the relevant Minister shall consult with the Commission during the process of the preparation of the legislative measure. GDPR Article 36.4 similarly requires that Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

(f) Given that some data is retained only for the purposes of compliance with the 2011 Act, and not otherwise processed by service providers for any

meaningful period of time, service providers are concerned that they will not be able to preserve this data on a retrospective basis. For example, should a District Court make a Preservation Order in respect of the location data of a named person, that person's location data up until the date of the making of the order would have already been deleted or anonymised. Service providers emphasise that Preservation Orders therefore must, at least in respect of certain data categories, be prospective only.

1.2 As the Joint Committee will easily discern, the points set out at (a) – (f) are not inconsequential. Each point listed provides for, and sets out, very significant and costly implementation challenges for the industry and State agencies listed in the 2011 Act in addition to the newly added State agencies now listed in the General Scheme.

1.3 The Joint Committee will also note that service providers and the broader industry are very aware of GDPR and Data Protection Act 1988 – 2018 legal compliance obligations which in a few instances, the said compliance obligations appear to jar with the intentions and aims of the General Scheme.

Dated the 29th day of June 2022

RONAN LUPTON SC

Chair at ALTO

JC2022/118

Three Ireland (Hutchison) Limited
Registered office

28/29 Sir John Rogerson's Quay,
Dublin 2

Registered Number: 316982
Place of Registration: Republic of Ireland

Three.ie

Alan Guidon
Clerk to the Committee
Committee on Justice
Leinster House
Kildare Street
Dublin
D02 XR20
justice@oireachtas.ie

29 June 2022

Re: Pre-Legislative Scrutiny of Communications (Retention of Data) (Amendment) Bill 2022 (the "Bill")

Dear Sir,

I understand the Committee on Justice (the "Committee") will be hearing submissions on the above Bill on Thursday 30th June 2022 and Three Ireland (Hutchison) Limited ("Three") would welcome the opportunity to make written submission to the Committee.

Three is Ireland's largest mobile telecommunications provider with 3.3 million customers and 40.7% market share. Three is owned by renowned global conglomerate CK Hutchison Holdings Ltd. The company has made close to €2 billion investment in building our business to date including €820 million in our Networks & IT infrastructure since acquiring O2 in 2014. Our annual overall investment is close to €100 million. Three has 1300 employees across retail, care, head office and data centres.

Since 2011, Three has invested in standalone, dedicated IT systems, processes and teams to deliver the requirements of the Communications (Retention of Data) Act 2011 (the "2011 Act"). Our government liaison unit works closely and collaboratively with the relevant law enforcement and other State bodies and has especially built a very strong co-operation between with An Garda Síochána to ensure an effective implementation of the 2011 Act. It Is our hope that we can continue to build on these positive relationships in compliance with our obligations under the proposed amendments to the 2011 Act.

Having had an opportunity to consider the contents of the General Scheme of the Bill provided by the Department of Justice on 21 June, we would like to raise some issues that we believe would benefit from further consideration and consultation between the Department of Justice, law enforcement agencies and the service providers:

Three Ireland (Hutchison) Limited
Registered office

28/29 Sir John Rogerson's Quay,
Dublin 2

Registered Number: 316982
Place of Registration: Republic of Ireland

1. There is a concern that the language surrounding the right to use the data retained for the purposes of National Security for responses to criminal investigation Preservation/Production Orders needs to be strengthened. Although, the General Scheme of the Bill provides for the creation of a table of definitions as to where Subscriber and Schedule 2 'Relevant Data' may be sourced from, at 7A.(10) and 7B.(9), and this includes "**data retained by a service provider under section 3 or 3A (The Data Retained for National Security Purposes)",** we would like for this to be more explicit. We have concerns about the alignment of this proposal with the recent Court of Justice of the European Union rulings on the topic of generalized retention of data. Ideally, we should be able to use the same IT system to respond to all the Order types.

2. The General Scheme of the Bill proposes to reduce the duration which data must be retained by service providers, compared to that required under the 2011 Act. We note however that the General Scheme does not provide for any transitional arrangements regarding the disposal of data which is held today under the 2011 Act. We would welcome provisions setting out the means and timelines by which service providers are obliged to delete data which is held in excess of the retention periods set out in the General Scheme of the Bill. In this regard we note that the General Scheme of the Bill would not at the date of commencement require the retention of any data, until or unless the appropriate court orders are sought and granted. Service providers are concerned that absent such orders being made, no legal basis would exist under Data Protection law for the ongoing retention of data currently retained under the 2011 Act. We note that much of the data currently retained is retained solely in order to comply with the 2011 Act and for no other purpose.

3. The General Scheme of the Bill at Sections 6B.(4), 6C.(3), 7A.(2), 7A.(4), 7A.(6), 7A.(8), 7B.(2), 7(B).(4), 7B.(6) and 7B.(8) provides for additional specified categories of data that may be required to be preserved and produced by service providers, as well as unspecified categories of data, being "such other class or classes [of data] as the member [or other relevant officer] may specify in the application". In relation to the new specified categories of data, it is anticipated that service providers would need to set up IT projects with anticipated twelve to eighteen month lead times to deliver the new IT functionality and processes to meet these requirements in a manner where they can be satisfied regarding the end to end integrity, completeness and lineage of the source data (which may be sourced from multiple IT systems) and its reproduction from machine readable to human readable formats in fulfillment of the applicable Preservation Order/Production Order. This is Three's experience of delivering complex data projects of this nature and is also the experience of

Three Ireland (Hutchison) Limited
Registered office

28/29 Sir John Rogerson's Quay,
Dublin 2

Registered Number: 316982
Place of Registration: Republic of Ireland

Three.ie

our sister companies in the Three Group in Europe where data retention regimes, similar to those contemplated by the Bill, are at more advanced stage of implementation. Where a Preservation/Production Order may require preservation or production of additional "classes [of data] as the member may specify in the application", service providers will be faced with unknown complexity and cost to fulfill such orders. Three would strongly recommend that Preservation/Production Orders be limited to the same categories of data retained under Section 3A (Schedule 2 Data). To the extent that it is necessary to include additional categories of data within the scope of Preservation/Production Orders, then these should be limited to those classes of data explicitly named in the Bill and the Bill, when enacted should, recognize the lead times faced by service providers to deliver on these requirements, by suspending the commencement of those provisions for up to eighteen/ twenty four months.

4. Three, in common with other service providers, is under a general obligation to limit the scope and duration of its processing of personal data to that which is required for its legitimate business purposes, after which, it is required to no longer process this data, consequently the categories of data and the period of time for which Three holds this data changes, as business needs and purposes evolve. There is, therefore, an industry concern it may not be possible for a service provider to comply with a Preservation Order to preserve categories of data from a period specified in such Order where this data is no longer retained for business purposes or is in the process of irreversible deletion.

5. In the context of the difficulties outlined above that may arise in service providers implementing the changes to the IT solution, and absent a suspension of the commencement of the relevant sections of the Bill when enacted, we are concerned that the offences provided by the General Scheme of the Bill are not appropriate during the initial period while the new IT systems and functionality are being put in place. Similarly, to the extent that a service provider is unable to preserve data from a period of time specified in an order because it legitimately no longer holds this data or can technically preserve it, then the Bill should provide that a service provider should not be liable, in that regard, for an offence for failing to comply with an Order.

6. In the context of the new order type and categories of information requests, we would request a statutory footing for a 'working group' or ministerial order to provide for collaboration with industry on the specific technical implementation and formats of the responses and the receipt and transmission of same. This would give a solid and transparent footing to the type of engagement that

Three Ireland (Hutchison) Limited
Registered office

28/29 Sir John Rogerson's Quay,
Dublin 2

Registered Number: 316982
Place of Registration: Republic of Ireland

happened in 2011 in the production of an implementation MOU between the operators and their State counterparts.

7. The General Scheme of the Bill does not explicitly close off routes of access to data other than via the data retention legislation itself, E.g. Section 50 of the Criminal Justice Act, 2007. Operators would welcome an explicit provision stating that they are not obliged to comply with such warrants or with a request for data made under any means other than those set out in the legislation.

If you have any questions, or if we may be of further assistance to clarify the above, please feel free to contact me directly.

Yours faithfully,

Patrick Foyle
Three Ireland (Hutchison) Limited