An Bille Cumarsáide (Sonraí a Choimeád) (Leasú), 2022
Communications (Retention of Data) (Amendment) Bill 2022

Meabhrán Míniúcháin
Explanatory Memorandum

AN BILLE CUMARSÁIDE (SONRAÍ A CHOIMEÁD) (LEASÚ), 2022

COMMUNICATIONS (RETENTION OF DATA) (AMENDMENT) BILL 2022

EXPLANATORY MEMORANDUM

Introduction

The purpose of the Bill is to amend the Communications (Retention of Data) Act 2011 ("the Principal Act") to ensure compliance with the rulings of the Court of Justice of the European Union in the area of general and indiscriminate retention of communications data for national security and law enforcement purposes. In general, the Bill provides for:

- updated rules on the general and indiscriminate retention of certain categories of communications data by communications service providers;
- two new types of legal orders, preservation and production orders, which allow for preservation and production of certain categories of communications data in individual circumstances, subject to judicial approval.

Provisions of the Bill

Section 1 is a standard provision confirming the title of the Bill.

Section 2 provides for a number of new definitions to be added to section 2 the Principal Act.

The term "Schedule 2 data" draws from the existing 2011 Act and is intended to capture traffic and location data. The approach ensures that only the minimum changes to the current data retention regime which are necessary to mitigate the impact of the recent Court of Justice rulings on data protection are introduced.

The term "internet source data" is introduced as a category of communications data already identifiable in the content of Schedule 2 of the Principal Act that are retained by service providers. This data can be used to identify IP addresses which may have accessed unlawful online content e.g. unlawful child abuse imagery. The retention of such data is not precluded by the Court of Justice rulings and a new system of specific retention and disclosure of such data is proposed for both law enforcement and security of the State purposes.

The term "user data" is proposed in section 2 instead of the term "subscriber data" which was proposed in the General Scheme of the Bill. "User data" captures all users of an electronic communications service, including not just subscribers (who may be party to a contract with a communications provider) but also other users, including those who may

enter and leave the jurisdiction and who e.g. for mobile telephony use data roaming services. The Court of Justice rulings do not preclude the continued retention of user data, which is already referred to in the existing Schedule 2 of the Principal Act.

Section 3

Section 3 amends the existing section 3 of the Principal Act, to provide for an obligation on service providers to retain "user data" for a period of 12 months. In this Bill, it is necessary to segregate the procedures governing retention of and disclosure of "user data" from the same procedures governing "Schedule 2 data" (which includes traffic and location data). The recent Court of Justice rulings do not require a change to the existing rules linked to the retention of user data, which has less of an impact on privacy rights. The net change for user data is that the retention obligation is confirmed as 12 months for all data within the meaning of that term. Provision is made for the Minister to vary this period to less than 12 months or a maximum of two years on stated grounds as he or she may consider necessary or proportionate.

Section 4

Section 4 provides for the insertion of new sections 3A and 3B into the Principal Act.

Section 3A provides for a new legal mechanism governing retention of Schedule 2 data. 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, he or 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 proportionate in all the circumstances to do so.

Section 3B provides for a standalone obligation to retain "internet source data" for a period of 1 year. Provision is made for the Minister to vary this period to less than 12 months or a maximum of two years on stated grounds as he or she may consider necessary or proportionate.

Section 5

Section 5 provides for the amendment of section 6 of the Principal Act. The new section 6 is intended to replicate, as far as user 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 to access user data retained by service providers.

Section 6

Section 6 provides for the insertion of new sections 6A to 6F into the Principal Act.

Section 6A 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.

Section 6B provides for a disclosure regime for an Garda Síochána and the Defence Forces to obtain access to Schedule 2 data in urgent circumstances, where there may not be time to seek approval by an

authorising judge. A system of post approval affirmation by an authorising judge within a set period of time of any such orders is provided for.

Section 6C provides for a regime of disclosure of retained internet source data on both law enforcement and state security grounds, where approved by an authorising judge.

Section 6D provides for a disclosure regime for an Garda Síochána and the Defence Forces to obtain access to internet source data in urgent circumstances, where there may not be time to seek approval by an authorising judge. A system of post approval affirmation by an authorising judge within a set period of time of any such orders is provided for.

Section 6E 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 of the Principal Act and is typically very recent data which is needed on an emergency basis by an Garda Síochána.

Section 6F provides for a single legal obligation on service providers to comply with the requirements to disclose data as set out in sections 6A to 6E above.

Section 7

Section 7 provides for the insertion of new sections 7A to 7D into the Principal Act.

Section 7A 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 specified Schedule 2 data 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. Service providers must, as the term suggests, preserve any Schedule 2 data listed in the order for a defined period.

Section 7B provides for "Production Orders", whereby an Garda Síochána, the Defence Forces, the Revenue Commissioners or the Competition and Consumer Protection Commission may seek the production of Schedule 2 data in specified cases 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. Data which may be obtained via a Production Order may already be the subject of a preservation requirement under section 7A. However, it will not be a condition of section 7B that the data concerned is already the subject of a preservation order.

Sections 7C and 7D provide 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. A system of post approval affirmation by an authorising judge within a set period of time of any such orders is provided for.

Section 8

Section 8 provides for the insertion of new sections 12A, 12B, 12C, 12D, 12E , 12F, 12G, 12H, 12I and 12J into the Principal Act.

Section 12A is an offence provision which will apply to all of the legal obligations for disclosure, preservation or production of data under the Bill. Penalties on summary conviction and conviction on indictment are listed.

This section 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.

Section 12B allows for the communications data terms in Schedule 2 of the Principal Act to be updated by regulation based on technology developments.

Section 12C provides for Ministerial guidelines on the operation of preservation and production orders.

Section 12D provides that data must be retained in an appropriate fashion to allow for disclosure.

Section 12E provides that any geographic criteria used to seek access to specific categories of data on a geographic basis must be non – discriminatory.

Section 12F provides for the making of regulations on a range of supplementary issues dealt with in the Bill.

Section 12G provides for the notification of relevant persons under certain circumstances where Schedule 2 data has been disclosed in respect of them. This does not apply where such data is disclosed on state security grounds.

Section 12H is a standard provision on service of documents.

Section 12I confirms that data processing under certain sections of the Bill will be in accordance with Part 5 of the Data Protection Act 2018.

Section 12J provides for the designation of "authorising judges" from the District Court, who will have the role of deciding on applications from an Garda Síochána, the Defence Forces, the Revenue Commissioners and the Competition and Consumer Protection Commission under the Bill.

Section 9

Section 9 introduces a new section 13A into the Bill. This is a transitional provision which allows for a time limited period where there can be disclosure, on state security grounds, of Schedule 2 data retained under the existing Principal Act.

Sections 10 and 11 provides for miscellaneous and consequential issues in the Bill, the short title and commencement.

An Roinn Dlí agus Cirt,

Iúil, 2022.

Wt. —. 250. 7/22. Essentra. (93095). Gr. 30-15.