Tithe an Oireachtais
Houses of the Oireachtas

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

Joint Committee on Justice, Home Affairs and Migration
Leinster House
Dublin 2

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

34/JC/06

17th December 2025

Mr Jim O'Callaghan TD,
Minister for Justice, Home Affairs and Migration,
51 St Stephen's Green,
Dublin 2, D02 HK52.

By e-mail to: ezbyrne@justice.ie

Our Ref: JC/7/1/G

RE: General Scheme of the Criminal Justice International Cooperation Office Bill 2025

Dear Minister,

I am writing to you in relation to the General Scheme of the *Criminal Justice International Cooperation Office Bill 2025* which was referred to the Committee for Pre-Legislative Scrutiny (PLS).

The Committee agreed to commence PLS by requesting an oral briefing from Departmental Officials on this matter.

On Tuesday 9th December 2025, the Committee received a 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 briefing, the Committee raised a number of questions with the officials. The Committee highlights the following concerns with the proposed legislation:

- What happens in cases where there are non-corresponding offences;
- The possibility of double-criminality, and whether Ireland will inadvertently contribute to poor human rights practices;
- Whether Ireland will be facilitating the prosecution of individuals who have committed an act or acts that here would not constitute a criminal offence;
- Whether AI be used to process applications;

- The lack of transparency as to how the State and providers will handle requests for data;
- The requirement for a publicly accessible register, providing information on requests received from other member states, how they requests are processed and the outcomes;
- The lack clarity and oversight regarding the role of the proposed office in reviewing data prior to its transfer;
- The lack of safeguards and incentives for providers to consider data protection rights and fundamental rights; and
- The lack of clarity around the staff of the proposed office and whether they will be required to have relevant legal expertise and experience.

In addition, the Committee is particularly concerned with:

- The ability to process a potential 300,000 cases per year (or 1,000 per day);
- The likely additional pressure on Courts;
- Whether a budget of €2.8 million and 30 staff will be sufficient in terms of resourcing, and whether this will negatively impact existing staff levels within the Department of Justice;
- The Committee has a fear that there is a very large and unquantifiable potential cost associated with this legislation.

In light of these concerns, the Committee sought written submissions from Dr TJ McIntyre and the Courts Service on the General Scheme. Dr McIntyre's submission is attached at Appendix 2, while the submission from the Courts Service can be accessed at Appendix 3.

In the submission, Dr McIntyre spoke about the following concerns he has with the proposed legislation, and accessing digital evidence in criminal matters:

- The lack of fundamental rights safeguards in the e-Evidence Package for those whose data is sought;
- The removal of many existing safeguards, which include
    - taking away the ability of a service provider to bring legal action to challenge abusive orders; and
    - providing that individuals can only challenge an order in the country where the order is made – not their home country;
- The lack of clarity around the admissibility of e-evidence;
- Whether legislation meets the standards articulated by the CJEU and the European Court of Human Rights (ECtHR) in relation to state surveillance;
- The lack of transparency and statistics around disclosure requests;
- Whether notifications will be issued to individuals subject to an access to data request and whether they will be able to challenge that request; and

- Whether, in the absence of reform, Irish law is capable of upholding privacy and data protection frameworks and protecting fundamental rights and the public interest in the effective investigation of crime.

Dr McIntyre believed this to be particularly concerning given democratic backsliding in EU Member States and increasing evidence of surveillance abuses, including use of spyware to target opposition politicians, journalists and civil society.

Dr McIntyre suggested the following recommendations to improve the proposed legislation and to promote fundamental rights:

- The mitigation of penalties where service providers act in good faith to protect data subject rights; and
- To require service providers to notify affected individuals.

While the Courts Service informed the Committee that it is due to engage further with the Department in the New Year, it stated that from its engagement to date, the impact of this General Scheme is limited as the majority of applications to the International Cooperation Office will need no involvement of a Court.

However, in relation to Head 4.7, the Courts Service noted that some appeals cases may be complex and could require significant court time, particularly where penalties involve substantial sums of money.

Regarding Head 4.8, the Courts Service believed that requiring a Court to confirm an uncontested decision by a new agency may not be the most efficient use of resources. The Service added that it is difficult to quantify the potential impact of the prosecution of new offences on the criminal courts.

The Courts Service also outlined concerns about the impact of the broader legislative programme in addressing data issues and also the outcome of the decision of the European Court in the Dwyer case. In its view, the central role that Courts are to play in managing applications relating to data access will need careful planning and resourcing if it is not to impact on other areas of Court activity.

The Committee recommends that serious consideration be given to the concerns raised in the course of its engagement on this matter as outlined in this correspondence.

The Committee acknowledges the constructive engagement by the Department; however, given the Department's own admission that this is the first time a system of this nature has been done, and the significant issues that remain unresolved, the Committee is of the view that the General Scheme would benefit from more thorough scrutiny, especially from a human rights perspective. The Committee recommends

that additional stakeholders should be afforded an opportunity to share their expertise on the matter prior to the Bill's progression to the Houses.

The Committee's preference was to conduct pre-legislative scrutiny hearings on this matter. However, due to the Minister's intention to publish the Bill early in 2026, the Committee must now conclude pre-legislative scrutiny on this General Scheme. The Committee looks forward to further engagement and debate on this Bill in the course of its consideration and passage through both Houses.

The Committee further agreed to publish the Department's opening statement as an appendix to this letter and lay it before both Houses. This is provided at Appendix 1 of this correspondence.

Dr McIntyre also submitted a copy of a recent chapter from the Cambridge Handbook of Digital Evidence in Criminal Investigations for context. This chapter follows Dr McIntyre's submission at Appendix 2.

Yours sincerely,

Matt Carthy

Matt Carthy TD
Cathaoirleach

APPENDIX 1

Opening Statement by the Department of Justice, Home Affairs and Migration at Committee meeting of 9th December 2025
General Scheme of the Criminal Justice International Cooperation Office Bill 2025
Joint Committee on Justice, Home Affairs and Migration

Background

E-evidence in the form of social media or electronic communications such as emails is now relevant in most criminal investigations. Within the EU, such services are frequently provided by one of the large service providers who may only have a physical presence in one of the member states. Traditionally jurisdiction was based on the physical presence of a body or evidence in that jurisdiction. However now a person residing in for example Belgium, who commits a crime in Belgium may be using electronic communications or social media provided by service providers based outside Belgium. What was once a local investigation now becomes an international one, and the traditional forms of judicial mutual assistance are quite complicated and take time.

To address this problem, the European Union adopted the e-Evidence package in July 2023. This is made up of:

- **Regulation** (EU 2023/1543) providing for European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal evidence, and
- **Directive** (EU 2023/1544) laying down rules harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

The **Regulation**, which has direct effect, provides for a system whereby a judicial authority in one member state (the issuing state) can order a service provider based in another member state (hosting state) to produce electronic evidence it possesses for the purpose of criminal investigations and proceedings. This is done without the need for any court order in the hosting state.

There are a number of safeguards in addition to the national law of the issuing state. The hosting state has to have an enforcing authority. In addition to its enforcing role it has a safeguarding role and in certain circumstances, it can intervene on its own initiative or at the request of the service provider and determine that an order should be refused for the grounds set out in the Regulation.

The **Directive,** which has to be transposed into Irish law, requires service providers offering services within the EU to formally designate at least one point of contact in a member state to receive and process orders made under the Regulation. Member states have to appoint central authorities to ensure that the requirements in the Directive are complied with and that authority must have the power to impose penalties on service providers for non compliance.

Purpose

The main purpose of the Bill is to give effect to the e-Evidence Directive and also provide for the central authority required by the Directive and the enforcement authority required by the Regulation. In an effort to avoid creating a new body, the Department spent some time exploring whether an existing body under the aegis of the Department or other Government Departments could carry out the tasks required. However no appropriate body could be identified. There are 3 key criteria that need to be met.

- The authorities will be facilitating the gathering of evidence for criminal investigations.
- The authorities have to be in a position to impose very significant administrative fines.
- The authorities have to cope with a large number of European Orders per annum.

I will just expand a little on these 3 criteria.

The e-Evidence package has taken a completely new approach to the gathering of e-evidence across borders. The traditional approach to gathering evidence in criminal proceedings would have required a request from a judicial authority in the issuing member state for a court order in the hosting state. The new EU approach does away with the involvement of the courts in the hosting state. There is no existing criminal justice body that is equipped to deal with the tasks required by the e-Evidence package.

The enforcement authority has to be in a position to make findings that a service provider is not in compliance with its obligations and has to be in a position to impose administrative fines up to 2% of total worldwide annual turnover (fines could exceed several billion euros).

A significant number of the largest social media and electronic communications service providers have their European presence in Ireland. Up to 600 service providers may designate a contact point in Ireland under the Directive. Ireland is likely to be responsible for the enforcement of the majority of all European Production Orders and in that role, a conservative estimate is that Ireland will receive in excess of 300,000 orders per annum.

As a result, on the third of June this year, the Government approved the establishment of a new body to act as the central authority and enforcement authority and also approved the priority drafting of a Criminal Justice (International Cooperation Office) Bill 2025. When approving the establishment of this new body, the Government took cognisance of the fact that this new body is likely to be given further tasks in the criminal justice area. Particular note was taken of the intention of the Minister to bring forward proposals to give effect to the Directive 2014/41/EU regarding the European Investigation Order in criminal matters.

Main Provisions of the Bill

Part 2 of the Bill provides for the establishment of the new body. There are very tight deadlines to be met. States are required to bring in laws by 18 February 2026 to give effect to the Directive (Article 7). Service providers have up to 18 August 2026 to designate their contact point (Article 3(6)) and notify the Central Authority. The Regulation applies with effect from 18 August 2026 (Article 34 (2)) and European Production Orders may be issued from that date, so the Irish enforcement authority has to be operational at that stage.

The legal structure chosen (Head 2.1) is that a person will be appointed Director and shall be a corporation sole with perpetual succession. The Director will have an office of staff to support him or her. To allow operations to start quickly, the onus will be on the Department to find office space, allocate staff and provide support in the IT, HR and Finance functions. The Director and staff of the office will be completely independent in the day-to-day decision making (Head 2.3).

The primary functions of the Director are in Head 2.4 and are to a large degree dictated by the EU Instruments.

Enforcing authority

The Regulation sets out the conditions for issuing orders. Orders must be necessary and proportionate (Articles 5.2 and 6.2) and respect the fundamental rights and legal principles enshrined in the EU Charter (Article 1.3).
There is an additional safeguard, where the offence did not take place in the issuing state or where the person whose data is sought does not reside in the issuing state, the enforcement authority must be notified and may raise grounds for refusal (Article 8). There is also a provision Article 10.5) where the service provider may raise issues with the enforcing authority.

In addition to the safeguarding role, the enforcing authority deals with non-compliance with an order and may issue significant fines. These are addressed in Part 4.

Central Authority

Under the Directive, the Director will have to oversee compliance by service providers with the following obligations:

- Service providers must designate a contact point within the EU for receipt of orders;
- The contact point must be properly resourced;
- Service providers must notify the details of the contact point and the languages used.

As the body responsible for ensuring compliance, the Director must coordinate with central authorities in other member states to ensure the Directive is applied in a consistent and appropriate manner.

Part 3 sets out the obligations of service providers, transposing them from the Directive. I have referred to the main ones above so I will not repeat them again.

Part 4 deals with sanctions. As mentioned above, the Directive will have to have the power to impose administrative sanctions under the Regulation and the Directive.

The procedure and the maximum fine to be imposed is set out in detail in the Regulation.

In the case of the Directive, it is a matter for Irish law. In both cases the procedures for imposing administrative fines are based on existing procedures set out in legislation. Part 8B of the Broadcasting Act 2009 as amended provides a model.

The Department is happy to answer any questions the members wish to raise.

APPENDIX 2

Digital Rights Ireland

Submission to Joint Committee on Justice, Home Affairs and Migration

General Scheme of Criminal Justice International Cooperation Office Bill 2025

1. Introduction

1.1 Digital Rights Ireland (DRI) thanks the Committee for the opportunity to make submissions on the General Scheme of the Bill.

1.2 DRI is in favour of increased international cooperation for access to data in criminal matters if this is done in a way which respects fundamental rights. In principle a clear legal basis is preferable to the largely unregulated practice of 'voluntary cooperation' which has developed among some providers.[1] Unfortunately the e-Evidence Package[2] has 'minimal fundamental rights safeguards'[3] for those whose data is sought. Instead, it takes away many existing safeguards: for example, it removes the ability of a service provider to bring legal action to challenge abusive orders, and provides that individuals can only challenge an order in the country where the order is made – not their home country. This is particularly concerning given democratic backsliding in Member States such as Hungary and increasing evidence of surveillance abuses, including use of spyware to target opposition politicians, journalists and civil society.[4]

1.3 While the e-Evidence Package is what it is, there are still some ways in which domestic legislation giving effect to the package can seek to promote fundamental rights and in this submission we suggest two additions to the General Scheme.

---

[1] T.J. McIntyre, 'Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, Their Irish Subsidiaries and European Legal Standards', in *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, ed. Federico Fabbrini et al. (Hart Publishing, 2021).

[2] Made up of two components: Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings ('e-Evidence Regulation') and Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings ('e-Evidence Directive').

[3] Jessica Shurson, 'The Balance of Efficiency and Fundamental Rights in the EU E-Evidence Regulation', *New Journal of European Criminal Law*, 3 August 2025, 20322844251357090, https://doi.org/10.1177/20322844251357090.

[4] Sophia in 't Veld, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware* (Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, 2023), https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

2. Mitigation of penalties where service providers act in good faith to protect data subject rights

2.1 Service providers face significant challenges in handling European Production Order Certificates ('EPOCs').[5] In emergency cases the provider will have only 8 hours in which to transmit data, even where an order is received in the middle of the night.[6] In other cases providers will have only 10 days.[7] Except for the very largest providers this creates a huge administrative burden.

2.2 These short time limits leave almost no time for providers to address difficult cases. Suppose, for example, a provider were to receive an abusive EPOC from Hungary for the emails of an investigative journalist. In that case the provider should seek to bring the matter to the attention of the Director of the Office for Criminal Justice International Cooperation,[8] who would then be responsible under Head 2.3 for determining whether to refuse the order. However, this is likely to involve significant delay in seeking legal advice as to what they can do – especially as this is a niche area where very few lawyers have any expertise – and may mean that they miss the deadline for transmission of data. In that case, the provider risks an exceptionally high fine – up to 2% of total worldwide annual turnover.[9]

2.3 This financial risk creates an incentive for providers simply to ignore fundamental rights concerns, particularly as they are given immunity for 'prejudice caused to their users or third parties that exclusively results from compliance in good faith with an EPOC' even if the EPOC later turns out to be invalid or abusive.[10]

2.4 We therefore suggest that Head 4.4 on penalties should be amended to include a provision mitigating penalties where a provider has acted in good faith to safeguard the rights of their users or affected third parties. As amended, Head 4.4(2) would read:

> (2) When determining the level of the penalty to be imposed, the Director shall take the following matters into account […]
>
> (b) The relevant circumstances should be taken into account, including
>
> (i) The nature, gravity and duration of the breach;
>
> (ii) Whether it was committed intentionally or through negligence,
>
> (iii) Whether the addressee has been held responsible for similar breaches previously and the circumstances concerned are indicative of repeated or systematic non-compliance.
>
> (iv) The financial strength of the addressee;

[5] Preservation orders are referred to by the acronym 'EPOC-PR'.
[6] E-Evidence Regulation, Article 10(4).
[7] E-Evidence Regulation, Article 10(3).
[8] E-Evidence Regulation, Article 10(5).
[9] E-Evidence Regulation, Article 15.
[10] E-Evidence Regulation, Article 15(2).

(v) If the addressee is a microenterprise, did failure to comply arise in an emergency case due to lack of human resources outside normal business hours;
(vi) Whether the addressee had reasonable grounds to believe, on the basis of specific and objective evidence, that the execution of an order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter. [Amendment underlined]

3. User notification

3.1 The most important safeguard in the e-Evidence Package is the obligation to notify individuals that their data has been accessed.[11] This then enables the individual to bring a challenge to the legality of the order and to raise a complaint with national data protection supervisory authorities.[12] Without notification, an individual is left unaware of illegal access to their data, and therefore also denied the right to an effective remedy under the ECHR and the Charter of Fundamental Rights.[13]

3.2 This obligation is contained in Article 13 of the e-Evidence Regulation, which provides as follows:

1. The issuing authority [i.e. the Member State seeking the data] shall, without undue delay, inform the person whose data are being requested about the production of data on the basis of a European Production Order.
2. The issuing authority may, in accordance with the national law of the issuing State, delay or restrict informing, or omit to inform, the person whose data are being requested, to the extent that, and for as long as, the conditions in Article 13(3) of Directive (EU) 2016/680 are met, in which case the issuing authority shall indicate in the case file the reasons for the delay, restriction or omission. A short justification shall also be added in the EPOC.
3. When informing the person whose data are being requested as referred to in paragraph 1 of this Article, the issuing authority shall include information about available remedies pursuant to Article 18.
4. The addressees and, if different, the service providers shall take the necessary state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved.

3.3 Article 13(1) of the e-Evidence Regulation therefore creates a rule that affected individuals must be notified of the fact that their data has been obtained, with an exception in

[11] E-Evidence Regulation, Article 13.
[12] E-Evidence Regulation, Article 18.
[13] See in particular the judgment of the Grand Chamber of the European Court of Human Rights *Roman Zakharov v Russia* App No 47143/06, Judgment, 4 December 2015, para 286 onwards.

Article 13(2) where disclosure would e.g. prejudice an ongoing investigation.[14] Where the issuing authority relies on this exception it must note this in the EPOC.

3.4 The difficulty with Article 13 of the e-Evidence Regulation is that it leaves notification of the person whose data has been obtained in the hands of the issuing authority seeking the data; leaving the fox in charge of the henhouse if these powers are being abused. The concern is that the issuing authority will delay notification, or simply not notify the individual.

3.5 We propose addressing this point by requiring service providers to notify affected individuals also, unless the issuing authority has asserted one of the exceptions to mandatory notification in the EPOC. Such notification is already common practice in the internet industry, and many large providers such as Apple, Facebook, Google and Yahoo already include an express commitment in their privacy statements to provide notification.[15] This provision would be codifying best practice across the industry.

3.6 We propose the following language, which is modelled on Head 10 of the General Scheme of the Criminal Justice (Protection, Preservation of and Access to Data on Information Systems) Bill 2024:[16]

Head 5 Duty to inform

Provide that:

(1) Where data has been disclosed to a person pursuant to a requirement under an EPOC, the addressee shall cause to be given to the person whose data has been requested a notice in writing informing him or her of the disclosure of the data concerned.
(2) Subsection (1) shall not apply if the issuing authority has added in the EPOC a justification for delaying, restricting informing, or omitting to inform, the person whose data has been requested.

3.7 To pre-empt a possible objection – it should be noted that such disclosure is not prohibited by Article 13(4) of the e-Evidence Regulation. That provision requires service providers to 'take the necessary state-of-the-art operational and technical measures to ensure

[14] Article 13(3) of Directive (EU) 2016/680 (Law Enforcement Directive) provides that 'Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject [...] to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others.'

[15] T-CY Cloud Evidence Group, 'Criminal Justice Access to Data in the Cloud: Cooperation with 'Foreign' Service Providers', Council of Europe, 3 May 2016, section 2.2.5, available at: https://rm.coe.int/168064b77d.

[16] Which is intended to give effect to Article 18 of the Budapest Convention and the e-Evidence Regulation in relation to domestic orders to produce specific data.

the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved'. On a superficial reading this might suggest that service providers are required to keep the existence of these orders confidential and secret as against the person whose data has been requested. However, such a reading would not be compatible with the obligation under Article 13(1) for the issuing authority to notify that person. If the issuing authority has not relied upon one of the exceptions under Article 13(2) then the fact of disclosure is not secret or confidential as against the person whose data has been requested.

Dr. TJ McIntyre
Chair, Digital Rights Ireland CLG

12 December 2025

12

Accessing Digital Evidence in Criminal Matters

An Inadequate Irish Legal Framework

T. J. McIntyre and Maria Helen Murphy[*]

12.1 INTRODUCTION

Ireland has become the location of the European headquarters and data centres of many of the world's largest internet firms, making it a key jurisdiction for police access to data held by various providers.[1] This was highlighted by the *Microsoft Ireland* litigation, which considered whether a United States court could require the production of data held in Ireland and saw the Irish government file an unprecedented amicus brief before the US Supreme Court asserting that the Ireland–US Mutual Legal Assistance Treaty (MLAT) should be used instead.[2]

Yet despite the importance of this sector to the Irish economy, there is little legislation in Ireland which deals with cross-border access to data or indeed access to data generally. Ireland has failed to ratify the Cybercrime Convention; it has opted out of the European Investigation Order (EIO); and the law on interception of communications predates the modern internet and remains largely unchanged since 1993.[3] For the most part, Irish practice in this area relies on older laws that are often ill-suited to digital material, with little case law to provide further guidance.

The one area where there has been modern legislation – telecoms data retention – was thrown into disarray by the April 2022 Court of Justice of the European Union (CJEU) judgment in the *Dwyer* litigation holding that the Communications (Retention of Data) Act 2011[4] was contrary to the ePrivacy Directive.[5] Legislation amending the 2011 Act[6] was controversially[7] rushed through in July 2022, but there remain significant question marks about the legality of the revised data retention regime.

[*] For their very helpful comments we thank Ronan Lupton, Denis Kelleher and another legal expert who has asserted their right to be forgotten. All errors are our own.

[1] The term 'provider' is used in this chapter as a catch-all covering the full gamut of internet services, including connectivity providers, webmail and messaging providers, hosting providers, domain name registrars, search engines, online gaming services and information society services generally.

[2] For context, see, e.g., Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 *Stanford Law Review Online* 9.

[3] See, e.g., the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

[4] Generally referred to in this chapter as 'the 2011 Act'. References to the 2011 Act are to the Act as amended most recently by the Communications (Retention of Data) (Amendment) Act 2022, the Criminal Justice (Miscellaneous Provisions) Act 2023 and the Policing, Security and Community Safety Act 2024.

[5] Case C-140/20, *G.D.* v. *Commissioner of An Garda Síochána and others* [2022] ECLI:EU:C:2022:258.

[6] Communications (Retention of Data) (Amendment) Act 2022.

[7] Karlin Lillington, 'Ireland's Slapdash Approach to Data Retention Legislation Sinks to New Low', *Irish Times*, 7 July 2022, www.irishtimes.com/technology/2022/07/07/irelands-slapdash-approach-to-data-retention-legislation-sinks-to-new-low/.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

This rickety legal framework is further weakened by reliance on voluntary disclosure of user data – where providers disclose data to police without any obligation to do so and without any specific legal framework regulating such requests.[8] In particular, Ireland – apparently uniquely among EU member states – permits providers to make voluntary disclosure of user data to foreign law enforcement.[9] The result is that there is little transparency as to how the Irish state and firms with an Irish presence handle requests for data, and in many cases there is a lack of fundamental rights safeguards against abuse.

In this chapter we consider these issues by discussing the ways in which Irish law regulates access to data for the purposes of criminal investigations, the cross-border arrangements in this area and the implications for effective law enforcement and fundamental rights.[10]

12.2 SETTING THE SCENE

12.2.1 *Collection of Digital Evidence*

To understand the Irish approach to the collection of digital evidence we must start with the fact that there is no general framework regulating access to data. The only technology-specific rules are those relating to interception of communications and data retention, under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and the Communications (Retention of Data) Act 2011, respectively. However, these apply only to messages transmitted by traditional operators such as landline, cable and mobile phone providers and internet connectivity providers.[11]

These Acts do not address over-the-top services such as WhatsApp, iMessage, or Snapchat, or search engines, social media providers, or other information society services and there is no Irish law specifically permitting access to data held by these types of providers. Consequently, it is important to bear in mind throughout this chapter that all references to 'interception of communications' and 'data retention' refer to laws that are limited to traditional telecommunications providers.

Apart from interception and data retention, Ireland does not have technology-specific rules and instead relies on the general law regarding search warrants and court orders to produce or give access to information ('production orders').[12] However, these powers are not consolidated in

[8] The nature and limits of this voluntary cooperation are considered in Section 12.4 in this chapter and in more detail in T. J. McIntyre, 'Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, Their Irish Subsidiaries and European Legal Standards', in Federico Fabbrini, Edoardo Celeste and John Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Oxford: Hart, 2021).

[9] See, e.g., Commission of the European Communities, *Non-paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, 15072/16, 2 December 2016, 1, 3–4, http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf.

[10] Two limitations should be noted. First, because this chapter focuses on the internet, we do not attempt to cover other sector-specific rules such as the exchange of information about financial transactions for criminal investigation purposes (regulated in part 2 of the Criminal Justice (Mutual Assistance) Act 2008). Second, the chapter considers access to data *for the purposes of the criminal law* – disclosures for national security purposes and emergency disclosures to safeguard lives are outside our scope.

[11] That is, 'authorised undertakings' as defined in the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2003 (SI 306 of 2003) and 'service providers' as defined in section 1 of the Communications (Retention of Data) Act 2011.

[12] Note that production orders are orders to produce documents or information already in being: a production order cannot be used to create an obligation to obtain new information.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

one place but are spread across a range of statutes and common law rules.[13] As Walsh puts it, 'current statutory powers to issue search warrants constitute an unwieldy collection of disparate provisions which have been developed in a piecemeal fashion over the past two centuries. Each authorises the issue of a search warrant only when its own peculiar requirements have been satisfied.'[14] The effect is that there are a range of rules regarding search warrants and production orders, depending on the type of crime being investigated, with differences such as:

- who can apply for a search warrant or production order;
- what offences can be investigated using a particular type of warrant/order;
- the evidential criteria to be met for the grant of a warrant/order;
- whether a person executing a warrant/order can require disclosure of a password necessary to operate a computer; and
- whether a person executing a warrant/order can require that information be decrypted.[15]

Recent pieces of legislation generally include specific provisions regarding the seizure of data. For example, section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 provides that search warrants issued under that Act include powers to seize computers and records, to operate computers at the place being searched, to require disclosure of passwords or encryption keys from a person at the place being searched and to require information stored on a computer to be produced in a visible and legible form.

However, older statutory powers of search and seizure do not have any similar provisions. For example, section 10 of the Criminal Justice (Miscellaneous Provisions) Act 1997[16] creates a catch-all power to issue search warrants in relation to any arrestable offence and is therefore one of the most used provisions.[17] But it is silent in relation to data. As a result, while a garda (police officer) carrying out a search under a section 10 warrant would be able to seize a computer and files, he or she would not be able to compel a person to reveal a password or to decrypt encrypted data.[18]

This reliance on the general law also means that (outside the areas of interception and data retention) there is no statutory power to compel providers to generate or log specific pieces of information. The search warrant and production order powers are static rather than dynamic – they are restricted to material which the provider already has and cannot be used to compel the provider to collect information on an ongoing basis.

The 2023 decision of the Supreme Court in *People (DPP)* v. *Patrick Quirke*[19] has highlighted the issues resulting from the lack of a specific legal regime regarding access to digital evidence. Quirke was convicted of murder based on circumstantial evidence which included evidence of internet searches on the decomposition of human remains found on a computer hard drive. In applying for a search warrant of his home, An Garda Síochána (the police force) failed to mention their intention to seize and examine his computer. As a result, the intention to search

[13] Maeve McDonagh and Micheál O'Dowd, *Cyber Law in Ireland* (Alphen aan den Rijn: Wolters Kluwer Law & Business, 2015), 384.

[14] Dermot Walsh, *Criminal Procedure* (Dublin: Thomson Round Hall, 2002), para. 8–09.

[15] For a general discussion of these differences, see, e.g., Law Reform Commission, *Report on Search Warrants and Bench Warrants* (Dublin, 2015), 47–74, www.lawreform.ie/_fileupload/Reports/Report%20on%20Search%20Warrants%20and%20Bench%20Warrants%201%20December%202015%20-%20Final%20Version.pdf.

[16] As amended by section 6 of the Criminal Justice Act 2006.

[17] 'Arrestable offence' is defined as an offence punishable by imprisonment of at least five years on conviction.

[18] It has been argued that this creates a gap in relation to crimes against children in particular. See, e.g., Geoffrey Shannon, 'Recommended Legislative Reforms on Child Protection', *ACJRD 19th Annual Conference: Cybercrime*, 7 October 2016, https://acjrd.ie/images/PDFs/annual-conference/19th_Annual_ACJRD_Conference_Report_Cybercrime.pdf.

[19] *DPP* v. *Patrick Quirke* [2023] IESC 5.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

the 'digital space apart from the physical space' was not put before the judge issuing the search warrant. The Supreme Court found that the search of digital devices was a particularly serious intrusion on privacy which required judicial analysis[20] of the proportionality of that search. The Supreme Court held that while the legislation permitted digital searches, the intention to seize and search digital devices must be brought to the attention of the judge issuing the search warrant if a search is to be lawful.[21] This meant that the search and seizure of Quirke's devices had been unlawful. However, in a subsequent decision as to the consequences of the ruling, the Supreme Court held that the police force had acted in good faith and could not have been expected to anticipate the novel legal finding regarding digital-space privacy in the principal *Quirke* ruling.[22] Consequently, the mistake in the search warrant application was found to be owing to 'honest inadvertence' and the criminal conviction was affirmed.[23]

12.2.2 *Admissibility of Digital Evidence*

Irish law takes a technology-neutral approach towards digital evidence by providing that the rules of evidence shall not exclude electronic evidence 'on the sole ground that it is an electronic communication, an electronic form of a document, an electronic contract, or writing in electronic form'.[24] As McGrath notes, Irish courts 'have not recognised electronic evidence as a distinct category of evidence requiring separate consideration or safeguards' and instead treat such evidence 'simply as a variety of documentary evidence, or sometimes as real evidence'.[25] Problems such as what constitutes the 'original' of a document produced on a computer have been addressed within that framework.[26] Digital evidence is also included within the documentary evidence system established by the Criminal Evidence Act 1992, which limits the hearsay rule and provides more lenient standards for the admissibility of business records.

Despite being admissible in principle, digital evidence presents problems in practice. Several cases have set a high threshold before digital evidence can be used. In *People (DPP)* v. *Meehan*,[27] the Court of Criminal Appeal summarised the position as follows: '[B]efore the judge can decide whether computer printouts are admissible, whether as real evidence or as hearsay, it is necessary to call appropriate authoritative evidence to describe the function and operation of the computer.' This requirement for 'appropriate authoritative evidence to describe the function and operation of the computer' proved difficult to meet when evidence was received from foreign service providers. In practice, it meant that detailed evidence was required from specialists in the relevant providers as to how their systems operated.[28] Some providers were willing to provide this additional evidence, but others were not, creating difficulties for prosecutors.[29]

[20] In accordance with *Damache* v. *DPP* [2012] IESC 11.
[21] *DPP* v. *Patrick Quirke* [2023] IESC 5.
[22] *DPP* v. *Patrick Quirke* [2023] IESC 20.
[23] This applied *DPP* v. *JC* [2017] 1 IR 417, a 2017 Supreme Court decision which overruled the previous legal position on unconstitutionally obtained evidence in Ireland.
[24] Electronic Commerce Act 2000, s. 22.
[25] Declan McGrath, *Evidence*, 2nd ed. (Dublin: Round Hall, 2014), 910. See, e.g., *DPP* v. *McD* [2016] IESC 71.
[26] McGrath, *Evidence*, 910.
[27] *DPP* v. *Brian Meehan* [2006] IECCA 104, relying on *R.* v. *Cochrane* (1993) Crim. LR 48.
[28] Michael Brady, 'Cyber-Crime, Confiscation, Disclosure, Mutual Legal Assistance and the Budapest Convention 2001, and Privacy Law In Ireland', *Fighting Cybercrime: Between Legal Challenges and Practical Difficulties*, 10–11 May 2016, 20–21, www.isrcl.com/wp-content/uploads/2021/05/Brady-Michael-Cyber-crime-confiscation-disclosure-mutual-legal-assistance-the-Budapest-Convention-2001-and-Privacy-law-in-Ireland.pdf.
[29] Ibid.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

This issue has been partially mitigated in relation to evidence from the USA. In September 2014 the Irish and US authorities agreed a revised form of certificate under the Ireland–US MLAT, which certifies the 'function and operation of the system' in relation to evidence which is automatically generated.[30] In *People (DPP)* v. *Moran*,[31] the Court of Appeal accepted that Facebook records of messages between users were admissible based on this certificate, without any further evidence being required. This makes the task of Irish prosecutors significantly easier in relation to evidence from the USA, but leaves the same issue in relation to evidence from elsewhere.[32]

12.2.3 *Data Retention Obligations*

12.2.3.1 Background

Irish data retention law has changed significantly in recent years. The law in this area is contained in the Communications (Retention of Data) Act 2011, which, as originally adopted, was a largely verbatim transposition of the Data Retention Directive[33] into Irish law.[34] However, it was clear after the 2014 judgment in *Digital Rights Ireland*[35] and the 2016 judgment in *Tele2*[36] that the 2011 Act failed to meet the standards of the Charter of Fundamental Rights and the European Convention on Human Rights (ECHR). In a 2017 report commissioned by the Department of Justice and Equality to review the law on data retention, the former Chief Justice, John Murray, found that

> the central finding in *Tele2* is clear: legislation providing for a system of general and indiscriminate communications data retention without exception is precluded by Article 15(1) of Directive 2002/58/EC. By the same token … it is also clear that the blanket data retention measures imposed by the Communications (Retention of Data) Act, 2011 are in essence indistinguishable from those impugned in *Tele2*.[37]

In that report, Murray also identified numerous other problems:

> The *principal* frailties of the 2011 Act … include: allowing statutory bodies an effective power of self-certification when making disclosure requests; failure to provide for prior independent authorisation of disclosure requests; failure to adhere to the clear statement principle by

[30] Ibid.

[31] *People (DPP)* v. *Moran* [2018] IECA 176.

[32] Though note the 2016 Supreme Court decision in *DPP* v. *McD* [2016] IESC 71, which suggests that the Irish courts may in the future reconsider the requirement for 'appropriate authoritative evidence' regarding digital evidence. In that case, the court held that there was no need for such evidence in relation to closed-circuit television (CCTV) footage, even when digitally recorded, as 'such devices have become ubiquitous in everyday life and their essential purpose and operation would be readily apparent to any reasonable person' (para. 55). The judgment also states that 'it may well be to over-read [*R.* v. *Cochrane*] even to say that it applies to all computers' (para. 54).

[33] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[34] For the Irish law prior to 2011, see T. J. McIntyre, 'Data Retention in Ireland: Privacy, Policy and Proportionality' (2008) 24(4) *Computer Law & Security Report* 326.

[35] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and others* [2014] ECLI:EU:C:2014:238.

[36] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and others* [2018] ECLI:EU:C:2016:970.

[37] John Murray, *Review of the Law on the Retention of and Access to Communications Data* (Dublin: Department of Justice and Equality, 2017), 44–45, 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; see also Data Protection Commissioner, *An Garda Síochána: Final Report of Audit* (March 2014), www.digitalrights.ie/wp-content/uploads/2014/07/Garda-data-protection-audit.pdf.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

> permitting undue legislative scatter of the rules governing data retention and disclosure; failure to articulate sufficiently clear objective criteria governing the conditions, circumstances and purposes surrounding data retention and disclosure; failure to provide clear procedures and protocols for the statutory bodies given a right of access to retained data; failure to make provision for the notification of persons affected, either directly or indirectly, by disclosure requests; failure to make appropriate provision for a remedy for wrongful access to retained data; failure to provide for the storage of retained data within the European Union.[38]

Despite this, official acknowledgement of the need for reform did not come until October 2017 when the Department of Justice and Equality published draft legislation to replace the 2011 Act.[39] However, that proposal itself still failed to meet the criteria set out in *Tele2* and was heavily criticised in pre-legislative scrutiny by the Oireachtas Joint Committee on Justice and Equality.[40]

In the meantime, the Irish state persisted with the use of data retention under the 2011 Act until finally forced to act by the CJEU judgment in *G.D.* v. *Commissioner of An Garda Síochána and others*[41] (better known in Ireland as the *Dwyer* case), which confirmed that the key elements of the 2011 Act were contrary to EU law. That judgment prompted the Irish government to push the Communications (Retention of Data) (Amendment) Act 2022 through Parliament in July 2022 as an emergency response with just four days of debate. This was extremely controversial; incredibly for a measure providing for mass surveillance, there was no public consultation, no prior consultation with the Data Protection Commission[42] and no data protection impact assessment, and Members of Parliament were not provided with the text in advance. This sudden exigency, long after Irish law was known to be in breach of EU law, is difficult to see as anything other than 'manufactured urgency in an attempt to sandbag any proper democratic scrutiny'.[43]

This manufactured urgency may have backfired on the state by making the 2022 Act unenforceable. Ireland failed to notify a draft of the 2022 Act to the European Commission[44] as required by the Technical Regulations Information System (TRIS) procedure,[45] with the result that the legislation will almost certainly be found invalid if challenged.[46] The state has attempted to mend its hand by a retrospective notification of the Act to the Commission under TRIS 'on

[38] Murray, *Review of the Law*, 115 (emphasis added).

[39] Department of Justice and Equality, *General Scheme of the Communications (Retention of Data) Bill 2017*, 3 October 2017, www.justice.ie/en/JELR/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf/Files/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf.

[40] Joint Committee on Justice and Equality, *Report on Pre-legislative Scrutiny of the Communications (Retention of Data) Bill 2017*, 32/JAE/22, January 2018, www.oireachtas.ie/parliament/media/committees/justice/2018/Data-Retention-Report-Final.pdf.

[41] *G.D.* v. *Commissioner of An Garda Síochána and others*.

[42] As required by the General Data Protection Regulation (GDPR) and the Law Enforcement Directive. See, e.g., section 84(12) of the Data Protection Act 2018 and Article 36(4) of the Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016, [2016] OJ L 119/1, 4 May 2016.

[43] Cormac McQuinn, 'Concern at "Rushed" Nature of Proposed Law to Deal With Fallout from Dwyer Appeal on Data', *Irish Times*, 30 June 2022, www.irishtimes.com/politics/oireachtas/2022/06/30/concern-at-rushed-nature-of-proposed-law-to-deal-with-fallout-from-dwyer-appeal-on-data/.

[44] Cianan Brennan, '"Illegitimate" Data Law Still Stands as EU Was Not Notified of New Act Rushed Through This Year', *Irish Examiner*, 4 December 2022, www.irishexaminer.com/news/arid-41021237.html.

[45] See Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services (codification), [2015] OJ L 241/1, 9 September 2015.

[46] Case C-194/94, *CIA Security International SA* v. *Signalson SA and Securitel SPRL* ECLI:EU:C:1996:172.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

a strictly precautionary and without prejudice basis'.[47] However, it is clear that only *draft* legislation may be notified under TRIS, making this belated notification of no legal effect.

The 2022 Act is, broadly speaking, a minimal response to the judgment in G.D. v. *Commissioner of An Garda Síochána and others*.[48] As discussed later, it maintains general and indiscriminate retention of traffic data and location data, addressing the CJEU jurisprudence by limiting the use of that retained data to state security purposes. It provides for general and indiscriminate retention of user data and internet source data for both state security and criminal law purposes. It also introduces, for the first time in Irish law, a preservation order (quick freeze) system in relation to telecommunications data. While in some regards the 2022 Act is an improvement over the 2011 Act, it nevertheless fails to address the majority of the recommendations in the Murray report and almost certainly fails to meet the standards articulated by the CJEU and the European Court of Human Rights (ECtHR) in relation to state surveillance. For example, the Act does not define what is meant by 'security of the state', does not provide explicit protection for journalists' sources and does not provide any judicial remedy to individuals for breaches.[49] It also fails to address concerns about the adequacy of the designated judge and complaints referee oversight mechanisms, which are discussed further in Section 12.4.5 of this chapter.

12.2.3.2 Legal Framework

The Communications (Retention of Data) Act 2011, as now amended by the Communications (Retention of Data) (Amendment) Act 2022,[50] applies only to 'service providers', defined as persons 'engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the Internet'.[51] The 2011 Act therefore covers traditional telecommunications providers only and does not apply to other services such as search engines, private networks, or over-the-top communications services such as WhatsApp or iMessage. There are no general data retention obligations in Irish law for those other services.

All service providers must retain 'user data', defined in section 1 of the Act to mean name, address, mobile phone number or fixed telephony phone number, international mobile subscriber identity (IMSI), international mobile equipment identity (IMEI), internet protocol (IP) address allocated by the service provider to the communication, user identity (ID), date and time of initial activation of service and date and time of last outgoing telephony communication.[52] This data must be retained on all users for one year.[53] Note, however, that the 2011 Act does not require registration for services such as prepaid subscriber identity module (SIM) cards – the obligation is to retain data already processed, not to process additional data, and services can still be provided anonymously.

All service providers must also retain 'internet source data', defined in section 1 of the Act to mean 'the IP address, whether dynamic or static, allocated by the service provider to the source of

47 Notification number 2022/872/IRL.

48 G.D. v. *Commissioner of An Garda Síochána and others*.

49 See, e.g., Irish Council of Civil Liberties, 'Why the Data Retention Bill Is So Problematic', 6 July 2022, www.iccl.ie/2022/why-the-data-retention-bill-is-so-problematic/.

50 Also note section 78 of the Criminal Justice (Miscellaneous Provisions) Act 2023, which addresses numerous drafting errors in the Communications (Retention of Data) (Amendment) Act 2022. Further changes are also made by the Policing, Security and Community Safety Act 2024.

51 Communications (Retention of Data) Act 2011, s. 1.

52 Ibid., s. 3.

53 The Minister for Justice may vary this period: Communications (Retention of Data) Act 2011, s. 3(2).

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

a communication [and] the name and address of the subscriber or registered user to whom an IP address was allocated at the time of the communication'.[54] This data must be retained on all users for one year.[55]

Retention of 'Schedule 2 data' – broadly speaking, the wider set of communications traffic data and location data – is regulated by section 3A. This permits the Minister for Justice to apply to a High Court judge *ex parte* (that is, in a closed hearing) for an order providing for general and indiscriminate retention of Schedule 2 data for twelve months. The judge may grant such an order if satisfied that it is necessary and proportionate for safeguarding the security of the state.[56] Where such an order is made, it applies to all service providers in respect of all users.[57] Such an order was made on 26 June 2023, to remain in force for one year. However, the order under section 3A may be renewed, and the assumption must be that there is an intention to keep this data retention in place indefinitely through rolling annual renewals.

12.2.3.3 Access to Data

User data can be accessed by An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Garda Síochána Ombudsman Commission (police disciplinary body).[58] Depending on the investigating body, user data may be accessed for the purpose of investigating an offence (not necessarily a serious offence) or a revenue offence, for national security purposes, for police disciplinary matters, for protecting the life or personal safety of a person or for determining the whereabouts of a missing person. A requirement to disclose user data is on the basis of internal authorisation by a senior official within each body – there is no requirement for authorisation by a judge or independent body.[59] There is no proportionality test in relation to disclosure of user data.

Internet source data can be accessed by An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Garda Síochána Ombudsman Commission.[60] Depending on the investigating body, user data may be accessed for the purpose of investigating a serious offence or a revenue offence, for national security purposes, for police disciplinary matters, for protecting the life or personal safety of a person or for determining the whereabouts of a missing person. Authorisation to require disclosure of internet source data is granted by a District Court judge, applying a test of necessity and proportionality.[61] However, in cases of urgency these bodies can access internet source data on the basis of internal authorisation by a senior official, followed by an application to a District Court judge for retrospective approval.[62]

[54] Communications (Retention of Data) Act 2011, s. 3B. Note that this overlaps with the definition of 'user data'.
[55] The Minister for Justice may vary this period: Communications (Retention of Data) Act 2011, s. 3B(2).
[56] Ibid., s. 3A(4).
[57] Ibid., s. 3A(5).
[58] Section 6 of the Communications (Retention of Data) Act 2011 as applied by section 98 of the Garda Síochána Act 2005. The Data Protection Commission can also authorise access (section 5). Service providers are prohibited from accessing data retained under the Act except where it is accessed: (a) at the request and with the consent of a person to whom the data relates, (b) for the purpose of complying with a disclosure request, (c) in accordance with a court order or (d) as may be authorised by the Data Protection Commissioner. The Act also provides for the extension of this and other powers to the Competition and Consumer Protection Commission in relation to competition offences, but at the time of writing these provisions have not yet been brought into force.
[59] Communications (Retention of Data) Act 2011, s. 6.
[60] Ibid., s. 6C as applied by s. 98 of the Garda Síochána Act 2005.
[61] Communications (Retention of Data) Act 2011, s. 6C(6).
[62] Ibid., s. 6D.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

Schedule 2 data can be accessed by An Garda Síochána and the Defence Forces for the purpose of state security.[63] Authorisation to require disclosure of Schedule 2 data is granted by a District Court judge, applying a test of necessity and proportionality.[64] However, in cases of urgency these bodies can access Schedule 2 data on the basis of internal authorisation by a senior official, followed by an application to a District Court judge for retrospective approval.[65]

Schedule 2 data which is being held by a service provider for a purpose other than compliance with a High Court retention order under section 3A (for example, for its own billing or quality assurance purposes) can be accessed for purposes other than national security, including investigation of serious offences and revenue offences.[66] The mechanism for doing so is a production order issued by a District Court judge on the basis of a test of necessity and proportionality.[67]

Cell site location data[68] (in essence, the most recent geographic location of a device) can be accessed by An Garda Síochána on the basis of internal authorisation for protecting the life or personal safety of a person or for determining the whereabouts of a missing person.[69]

12.2.3.4 Data Preservation

Irish law does not generally provide for data preservation (quick freeze) orders in relation to criminal investigations. However, the 2011 Act permits An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Garda Síochána Ombudsman Commission to apply to a District Court judge for a preservation order in relation to Schedule 2 data.[70] This may be done for investigating a serious offence or a revenue offence, for national security purposes, for police disciplinary matters, for protecting the life or personal safety of a person or for determining the whereabouts of a missing person. Those bodies may also issue a temporary preservation order based on internal authorisation in cases of urgency.[71]

12.2.3.5 Voluntary Disclosures

Outside the 2011 Act, Irish police adopted a parallel tactic of obtaining telecommunications data on a voluntary basis. This practice developed in reliance on section 8 of the Data Protection Acts 1988–2003 which disapplied data protection restrictions on processing personal data where processing was 'required for the purpose of safeguarding the security of the State' or 'required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders … [if] the application of those restrictions would be likely to prejudice [this enforcement]'.[72] While this did not

[63] Ibid., s. 6A.
[64] Ibid., s. 6A(4).
[65] Ibid., s. 6B. See also sections 7C and 7D, which create overlapping powers to seek production orders in relation to Schedule 2 data that is being stored by a service provider for purposes other than compliance with a retention order under section 3A.
[66] Communications (Retention of Data) Act 2011, s. 7C.
[67] Ibid., s. 7C(8).
[68] Defined in section 6E(5) of the Communications (Retention of Data) Act 2011 to mean 'data processed by means of an electronic communications network that identifies the most recent geographic location of the device or equipment used by a user when availing of a publicly available electronic communications service'.
[69] Communications (Retention of Data) Act 2011, s. 6E.
[70] Ibid., s. 7A, as applied by section 98 of the Garda Síochána Act 2005. There is a parallel scheme of 'temporary production orders' under section 7D.
[71] Communications (Retention of Data) Act 2011, s. 7B.
[72] This section has since been replaced by section 41 of the Data Protection Act 2018.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

compel providers to disclose data, or provide a legal basis for police to request such data, it was nevertheless frequently used by police to obtain data for matters outside the scope of the 2011 Act, such as minor offences, sidestepping the safeguards in that legislation in a way that clearly contravened EU law and ECHR standards.[73] While the Murray report should have put an end to this practice, there are anecdotal reports that similar requests continue to be made. Service providers should be aware that disclosure of user data without a statutory basis is in breach of section 5 of the 2011 Act.

12.2.3.6 Notification, Redress and Judicial Oversight

Section 12G of the 2011 Act provides for notification of individuals that Schedule 2 data relating to them has been disclosed, except where the disclosure is for state security purposes. There is no provision for notification of disclosure of user data, internet source data or cell site location data. There is limited provision for investigation and redress in case of wrongful access to data by the state through a complaints referee mechanism,[74] and there is provision for oversight by a designated judge of the High Court.[75] These are considered in detail in Section 12.4.5 of this chapter.

12.3 TERMINOLOGY AND CATEGORISATIONS

12.3.1 *Data*

12.3.1.1 Terminology

There is no general definition of 'data' in Irish criminal procedure; the only specific references to 'data' appear to be in the Communications (Retention of Data) Act 2011, where 'data' is defined as 'traffic data or location data and the related data necessary to identify the subscriber or user',[76] and in the Criminal Justice (Offences Against Information Systems) Act 2017, where 'data' is defined as 'any representation of facts, information or concepts in a form capable of being processed in an information system, and includes a programme capable of causing an information system to perform a function'.[77] However, those definitions apply only within the context of each Act – not more generally.

Instead, legislation dealing with search warrants, production orders and evidence generally refers to 'documents', 'records' or 'information', with these terms typically being defined to include computer data also. For example, section 7(4) of the Criminal Justice (Offences Relating to Information Systems) Act 2017 gives the power to issue search warrants which allow police to:

> (a) operate any computer at the place that is being searched or cause any such computer to be operated by a person accompanying the [police officer] for that purpose, and
> (b) require any person at that place who appears to the [police officer] to have lawful access to the information in any such computer—

[73] See, e.g., Murray, *Review of the Law*, 44–45; Data Protection Commissioner, 'An Garda Síochána', 61–62.
[74] Communications (Retention of Data) Act 2011, s. 10.
[75] Ibid., s. 11.
[76] Ibid., s. 1.
[77] Criminal Justice (Offences Against Information Systems) Act 2017, s. 1.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

(i) to give to the [police officer] any password necessary to operate it and any encryption key or code necessary to unencrypt the information accessible by the computer,
(ii) otherwise to enable the [police officer] to examine the information accessible by the computer in a form in which the information is visible and legible, or
(iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.[78]

12.3.1.2 Categorisation

Just as there is no general definition of 'data' in Irish criminal procedure, there is no general classification or regulation of *types* of data. For example, there is no specific categorisation or regulation of access to unread emails, draft emails, chat rooms, communication in the context of online games, domain name registration details or machine-to-machine data.

There is a content/metadata distinction in the context of telecommunications surveillance under the interception and data retention regimes. Mandatory interception of the content of relevant telecommunications messages requires a warrant signed by the Minister for Justice under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, while police access to metadata is governed by the Communications (Retention of Data) Act 2011 and may require judicial approval, depending on the type of metadata involved and the purpose for which it is sought.[79] The Communications (Retention of Data) (Amendment) Act 2022 has recently introduced distinct categories of 'internet source data', 'cell site location data' and 'user data' with different rules applying to each (see Section 12.2.3).

12.3.2 *What Services Are Covered? 'Service Providers' and 'Authorised Undertakings'*

As already noted, Irish interception and data retention laws apply only to traditional telecoms providers such as mobile phone or broadband providers. Specifically, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 applies to messages being transmitted by 'authorised undertakings', while the Communications (Retention of Data) Act 2011 applies to 'service providers'.[80] In both cases, therefore, over-the-top services and other information society services do not fall within the scope of this legislation.

[78] This power raises issues as to whether compelled disclosure of a password might violate the privilege against self-incrimination, but the Irish courts have yet to address this point. Compare Orin S. Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination' (2019) 97 *Texas Law Review* 767; and Caren Myers Morrison, 'Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment' (2012) 65 *Arkansas Law Review* 133. The Irish authorities have stated that 'prosecution for withholding passwords is generally not done due to the right against self-incrimination': Council of the European Union, *Evaluation Report on the Seventh Round of Mutual Evaluations – The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime: Report on Ireland*, 7160/1/17, 2 May 2017, 68, http://data.consilium.europa.eu/doc/document/ST-7160-2017-REV-1-DCL-1/en/pdf.

[79] Section 2 of the Communications Act 2011 provides that '[t]his Act does not apply to the content of communications transmitted by means of fixed network telephony, mobile telephony, Internet access, Internet e-mail or Internet telephony'.

[80] 'Authorised undertakings' as defined in the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2003 (SI 306 of 2003) and 'service providers' as defined in section 1 of the Communications Act 2011.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

In 2016 the Department of Justice and Equality announced plans to extend the interception regime to over-the-top services also. According to the policy document:

> Communications services delivered over the internet are not covered by the current legislation as the powers of direction currently vested in the Minister for Communications are effectively restricted to Telecoms and Postal Service providers. This means that communications services such as those provided by the major Internet based entities cannot be made subject to the legislation. In addition, the terminology in the Act of 1993 does not adequately reflect the modern face of communications, particularly where defining 'communications' and communications addresses is concerned. As the legislation stands Ireland can only comply to a limited extent with requests from other EU Member States for mutual legal assistance where interception is concerned. The fact of the matter is that mobile devices are now used to communicate in a much wider array of ways than simply by texting or holding a telephone conversation. The legislation has not kept pace with these developments and needs to be changed.[81]

This proposal was light on detail, but essentially proposed that the existing interception framework[82] should be extended to information society services, including search engines and social media.[83] However, it was clear that the plan to simply extend the existing interception regime was not credible; the legal framework for interception lacks the basic safeguards (such as independent judicial authorisation and controls on use of intercepted data) necessary to ensure compliance with the ECHR and the Charter of Fundamental Rights.[84] There have been no further public updates since this proposal was published and it appears to have stalled, possibly owing to significant pushback from the internet industry, which has demanded that any new law should provide for significant reform to include judicial authorisation of interception.[85]

12.4 DOMESTIC COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

12.4.1 *Introduction*

Access to data held by providers has historically been extremely common in Irish criminal investigations. The main type of data accessed is that held by traditional telecoms providers: state agencies requested communications data (mobile, landline and internet) approximately 92,200 times over the period from 2013 to 2017 inclusive, roughly 18,450 times each year on average.[86] The Garda Síochána (police force) was by far the biggest user of this information at 90,200 requests, followed by the Defence Forces (1,380), the Garda Síochána Ombudsman

[81] Department of Justice, 'Policy Document on Proposed Amendments to the Legislative Basis for the Lawful Interception of Communications'.

[82] Postal and Telecommunications Services Act 1983, s. 110.

[83] As defined in EC Directive 98/34/EC of the European Parliament and Council laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services, OJ L 204, 21 July 1998, p. 37, and paragraph 18 of the Preamble of Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce), OJ L 178, 17 July 2000, p. 1.

[84] See, in particular, Maria Helen Murphy, 'The Analytical Approach of the European Court of Human Rights in Surveillance Cases: The Implications, Justifications, and Future of the Court's Reasoning, with a Focus on the Legislative Impact in Ireland', PhD thesis, University College Cork (2013), ch. 5.

[85] See, e.g., Wayne O'Connor, 'New Laws to Monitor Criminal Messaging Risk Pushing Out Technology and Social Media Firms', *Irish Independent*, 19 November 2017, www.independent.ie/irish-news/new-laws-to-monitor-criminal-messaging-risk-pushing-out-technology-and-social-media-firms-36333077.html.

[86] Cormac O'Keeffe, 'Personal Data Shared 92,000 Times to State Agencies by Phone and Internet Firms', *Irish Examiner*, 10 December 2018, www.irishexaminer.com/opinion/commentanalysis/arid-30890965.html.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

Commission (440) and the Revenue Commissioners (150). Of the Garda requests, approximately half were for subscriber data (such as name and address of a subscriber) and half for call and internet data (such as numbers called and phone location history). However, the number of requests fell dramatically in the period between the CJEU judgment in *G.D.*[87] and the bringing into force of the Communications (Retention of Data) (Amendment) Act 2022, with just 299 Garda requests from January to May 2023.[88]

Access to other forms of data is not as ubiquitous but is still common. There are no official statistics on this point, but transparency reports published by Microsoft, Facebook, Google and Twitter indicate that a total of 1,259 disclosure requests were made by state agencies over the period from 2013 to June 2018.[89] Requests to smaller and domestic providers are harder to gauge, as many do not publish transparency reports, but it is clear that the number of these requests is on the increase.[90] Transparency reports do not usually identify the legal basis for requests, but many of these appear to be requests for voluntary disclosure.[91]

12.4.2 *Distinction between Domestic/National and Cross-Border/Transnational Situations*

Irish law does not draw a general distinction between domestic/national and cross-border/transnational situations in relation to access to data. The rules that determine whether data can be accessed by a compulsory process depend on the legislative language creating each power.

12.4.3 *Nature of the Cooperation*

Police access to information held by providers in Ireland is based on a mix of mandatory and voluntary cooperation. In this section we consider the legal framework for mandatory cooperation (where there is a legal basis for the cooperation of providers who can be *compelled* to provide information) and voluntary cooperation (where providers cannot be *compelled* to provide information and there may or may not be an explicit legal basis *permitting* them to do so).

12.4.3.1 Mandatory Cooperation

There is no general legal basis for mandatory cooperation: as we outlined in Section 12.2.1, Irish law provides different rules in respect of each type of investigative measure. Consequently, the main investigative powers – interception of communications, access to retained data, search warrants and production orders – differ widely on the basic criteria: What state bodies may seek data? From what types of providers? For what purposes? In respect of what types of crime? Using what type of authorisation? These powers are outlined in Section 12.4.4.

Data obtained through mandatory cooperation is capable of being used as evidence, subject to the ordinary rules of admissibility. In practice, the Irish state has a long-standing policy against using communications intercept evidence (evidence obtained under the Interception of Postal

[87] *G.D.* v. *Commissioner of An Garda Síochána and others.*

[88] Cianan Brennan, 'Garda Requests for Phone Records Down Dramatically Since New Law Was Enacted', *Irish Examiner*, 15 January 2024, www.irishexaminer.com/news/courtandcrime/arid-41308759.html.

[89] Cormac O'Keeffe, '1,250 Requests to Access Private Data', *Irish Examiner*, 26 November 2018, www.irishexaminer.com/news/arid-30887779.html.

[90] See, e.g., Michele Neylon, 'Increasing Transparency', Blacknight Blog, 14 June 2018, https://blacknight.blog/increasing-transparency.html.

[91] See, e.g., McIntyre, 'Voluntary Disclosure of Data to Law Enforcement'.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

Packets and Telecommunications Messages (Regulation) Act 1993) in prosecutions, apparently to avoid revealing details of this intercept capability.[92] It is important to note that this policy does not extend to communications which are obtained other than through the 1993 Act – for example, messages which have been obtained from a seized mobile phone are frequently used in evidence.

Any mandatory cooperation requirement can in principle be challenged either by the provider or by the individual whose data is sought. For example, in *CRH Plc, Irish Cement Ltd & others* v. *The Competition and Consumer Protection Commission*, one of the plaintiffs challenging a warrant that authorised search of the Irish Cement Limited premises was an executive who successfully claimed that seizure of his entire email account was disproportionate.[93] The admissibility of evidence obtained in this way can also be challenged by a defendant in any subsequent criminal trial, and the Irish exclusionary rule will mean that such evidence may be excluded if it was obtained illegally or unconstitutionally.[94]

To challenge access to data the individual must, of course, be aware of the fact that their data has been sought. However, Irish law does not generally provide for any such notification to individuals.[95] This gap is only partly remedied by the policies of some of the major providers (such as Apple, Facebook, Microsoft and Yahoo) which commit to notifying users where their data is sought, with some exceptions.[96]

The extent of the obligations imposed on providers varies as between interception, data retention and search warrants/production orders. In the case of search warrants/production orders, the obligations imposed are relatively straightforward – to cooperate with a search at a particular place, provide decryption or login information or produce certain information by a particular time.[97] In the context of data retention, providers are obliged to retain data so that it can be disclosed without delay[98] and the Minister for Justice may impose additional technical requirements in relation to data quality.[99] The position is opaque in relation to interception, where there is no public information as to the content of warrants under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 or the underlying ministerial directions these warrants rely upon, and no details as to whether there is a time limit for compliance or what other obligations might be imposed on authorised undertakings.

The format in which data must be provided varies. In relation to data retention, the Communications (Retention of Data) Act 2011 provides an extensive list of information to be retained and provided. In the case of search warrants and production orders, the statutory powers do not require provision of information in any particular format except to the extent that some powers may require decryption of information and provision of information in a form in which

[92] Justice, *Intercept Evidence: Lifting the Ban* (London: Justice, 2006), 56–57, https://files.justice.org.uk/wp-content/uploads/2015/07/06170838/Intercept-Evidence-1-October-2006.pdf.

[93] *CRH Plc, Irish Cement Ltd & ors* v. *The Competition and Consumer Protection Commission* [2017] IESC 34.

[94] On the extent of this rule and judicial discretion to admit unconstitutionally obtained evidence, see Yvonne Marie Daly, 'Overruling the Protectionist Exclusionary Rule: *DPP v JC*' (2015) 19(4) *International Journal of Evidence & Proof* 270.

[95] Except in relation to Schedule 2 data under the Communications (Retention of Data) Act 2011.

[96] The T-CY Cloud Evidence Group, *Criminal Justice Access to Data in the Cloud: Cooperation with 'Foreign' Service Providers* (Strasbourg: Council of Europe, 3 May 2016), s. 2.2.5, https://rm.coe.int/168064b77d.

[97] In practice, seven days seems to be the norm for compliance with a search warrant or production order. See, e.g., US Supreme Court, *United States of America v. Microsoft Corporation on Writ of Certiorari to the United States Court of Appeals for the Second Circuit, Joint Appendix* (2017), 37, www.supremecourt.gov/DocketPDF/17/17-2/22918/20171206204555098_United%20States%20v.%20Microsoft%20Joint%20Appendix.pdf.

[98] Communications (Retention of Data) Act 2011, s. 12D(a).

[99] Ibid., s. 12F(2)(a).

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

the 'information is visible and legible'. In relation to intercept material, it may be that ministerial warrants and directions to telecommunications providers prescribe the format in which data is to be provided, but there is no public information as to the content of these directions.

Failure to comply with an interception warrant, search warrant, production order, retention obligation or disclosure requirement will constitute an offence, subject in some cases to defences of reasonable excuse or due diligence.[100] These statutory powers do not define these defences further and it is not clear whether the defences would include reasons such as conflicting legal obligations or excessive costs of compliance.[101]

12.4.3.2 Voluntary Cooperation

In addition to mandatory disclosure, Irish police rely on voluntary cooperation by providers.[102] We have already seen this in the context of data retention (in Section 12.2.3), where there is a questionable practice of seeking telecommunications data in situations where disclosure would not be permitted under the Communications (Retention of Data) Act 2011.[103] Requests for voluntary disclosure can be used for other data also if providers are willing to cooperate – for example, Ireland's leading domestic hosting provider and domain name registrar states in its law enforcement guidelines that it will provide user information on the basis of 'a valid request signed by a Garda Superintendent or higher rank'.[104]

12.4.3.3 Historical Development of Voluntary Disclosure

Voluntary disclosure initially developed on the basis of section 8 of the Data Protection Acts 1988 and 2003 (which has since been repealed by the Data Protection Act 2018). Section 8(b) disapplied restrictions in the Data Protection Acts if processing was 'required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders . . . in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid'. This section was, however, deeply problematic. It did not *authorise* disclosure or regulate it; it merely disapplied restrictions imposed by the Data Protection Acts. Restrictions imposed by other legislation or legal rules (such as obligations of bank secrecy or professional confidentiality) were not affected. It made it the responsibility of the data controller to determine if disclosure is necessary and proportionate – effectively outsourcing what should be a public law function.[105] In particular, it was insufficient to regulate access to communications data as it did not meet the criteria elaborated by the CJEU in *Digital Rights Ireland* and subsequent cases.[106]

[100] See, e.g., section 110 of the Postal and Telecommunications Services Act 1983 as amended by section 30 of the Criminal Justice (Mutual Assistance) Act 2008, section 15 of the Criminal Justice Act 2011 and section 12A of the Communications (Retention of Data) Act 2011.

[101] The reasoning in *Walsh* v. *National Irish Bank* [2013] IESC 2 suggests that a provider might have a defence if compliance would put it in breach of its legal obligations in another jurisdiction; however, that case concerned data held in another jurisdiction and it is not clear that the same reasoning would be applied in respect of data held in Ireland.

[102] See, e.g., McIntyre, 'Voluntary Disclosure of Data to Law Enforcement'.

[103] Murray, *Review of the Law*, 44–45; Data Protection Commissioner, 'An Garda Síochána', 61–62.

[104] 'Law Enforcement Guidelines', Blacknight Solutions, n.d., www.blacknight.com/legal/law-enforcement-guidelines/.

[105] Data Protection Commissioner, 'Disclosures Permitted under Section 8 of the Data Protection Act', n.d., https://web.archive.org/web/20130607050018/https://www.dataprotection.ie/docs/Disclosures-Permitted-under-Section-8-of-the-Data-Protection-Act-Section/237.htm.

[106] See, e.g., Denis Kelleher, *Privacy and Data Protection Law in Ireland*, 2nd ed. (Haywards Heath: Bloomsbury Professional, 2015), 95.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

Despite these limitations, the section came to be extensively used by providers. This was first brought to public attention by the Data Protection Commissioner audit of Facebook Ireland in 2012. That audit examined requests from law enforcement agencies to Facebook for user data, and accepted Facebook's assessment that it was entitled to disclose non-content data in response to both Irish and foreign police requests, including to law enforcement agencies outside the European Economic Area (EEA), on the basis of a case-by-case examination of each request.[107]

This tiered approach – giving voluntary disclosure of non-content data but requiring a mutual legal assistance request or other mandatory process for content data – echoes the content/non-content distinction under US law in the Stored Communications Act.[108] Perhaps unsurprisingly, other major US providers appear to have carried over the same approach to their Irish operations. In a 2016 report, the Council of Europe Cybercrime Convention Committee surveyed the law enforcement guidelines of Apple, Facebook, Google, Microsoft, Twitter and Yahoo.[109] All bar Google and Yahoo identified Irish law as applying to at least some of the information they hold, and all of those firms drew a distinction between non-content data and content data, with the former being made available on the basis of a 'valid legal request' and the latter requiring a mutual legal assistance request or other binding legal process. That survey is now out of date, but the underlying result is significant – all the firms holding user data in Ireland appeared to take the view that they could disclose (non-content) user data without a mandatory requirement to do so under Irish law, at least in some circumstances.

12.4.3.4 Is Voluntary Disclosure Permitted after the GDPR?

The already problematic basis for voluntary disclosure has become even more dubious since the General Data Protection Regulation (GDPR) was implemented in Irish law. Section 8 of the Data Protection Acts 1988 and 2003 no longer applies, and the closest provision is section 41 of the Data Protection Act 2018, which provides:

> [T]he processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—
>
> (a) of preventing a threat to national security, defence or public security,
> (b) of preventing, detecting, investigating or prosecuting criminal offences.

The Data Protection Commission has asserted that this provides a legal basis for voluntary disclosure of data by controllers to police, though it has not given any detailed guidance on the point.[110] But even on a preliminary assessment there are problems with this approach.

Despite a superficial resemblance, the legal effect of section 41 of the 2018 Act is quite different from that of section 8 of the Data Protection Acts 1988 and 2003. Section 41 does not completely disapply other data protection rules as the previous section did. Nor can it provide

[107] Data Protection Commissioner, *Facebook Ireland Report of Audit* (21 December 2011), 98–100, appendix 5, www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf; Data Protection Commissioner, *Facebook Ireland Ltd Report of Re-audit* (21 September 2012), 34–36, www.europe-v-facebook.org/ODPC_Review.pdf.

[108] Data Protection Commissioner, *Facebook Ireland Report of Audit*, appendix 5.

[109] The T-CY Cloud Evidence Group, *Criminal Justice Access to Data in the Cloud*.

[110] Data Protection Commission, *Guidance for Drivers on Use of 'Dash Cams'* (2018, updated December 2019), www.dataprotection.ie/sites/default/files/uploads/2019-12/GuidanceforDriversontheuseofDashCams.pdf.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

a free-standing legal basis for processing (given that the grounds in Articles 6 GDPR are exhaustive). Instead, section 41 merely permits processing for a purpose other than that for which the personal data was collected. This is supported by the legislative history; in a parliamentary committee, the Minister for Justice and Equality stated that section 41 was intended to provide a basis for other '[s]tatutory provisions that permit, or require, further notification of disclosure of personal data', such as obligations to report money laundering or child abuse.[111]

Notwithstanding section 41 of the 2018 Act, therefore, voluntary disclosures of personal data to law enforcement still require a specific legal basis to comply with Article 6 GDPR (and Article 9 GDPR in the case of special category data). A full assessment of the power to make voluntary disclosure is beyond the scope of this chapter, but it is fair to say that it is a considerably more complex issue than the rather simplistic approach apparently endorsed by the Data Protection Commission.[112]

For example, in many cases of voluntary disclosure the legal basis will be the legitimate interest of the controller. In this context, a balancing test must be used which requires an individualised assessment of the need for disclosure and the impact on the data subject.[113] A blanket policy of disclosing data in response to police requests will be contrary to the GDPR. Similarly, Recital 50 GDPR makes it clear that voluntary disclosure on the basis of legitimate interest cannot be relied upon if there is a countervailing obligation of secrecy in a particular case:

> Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. *However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy*.[114]

In practical terms, therefore, the GDPR makes an important change which should force providers with an Irish presence to reconsider voluntary disclosure practices they developed under the prior legislation; providers will be at real risk if they make voluntary disclosures without a clear legal basis for doing so, which section 41 of the Data Protection Act 2018 does not provide.[115]

[111] Charlie Flanagan TD, Oireachtas Select Committee on Justice and Equality, 3 May 2018.

[112] See, e.g., Thomas Kopp and Valentin Pfisterer, 'Between a Rock and a Hard Place: Legal Pitfalls of Voluntary Cooperation of German Companies with German and Foreign Regulatory and Law Enforcement Authorities' (2016) 2(2) *Compliance Elliance Journal* 24; Clare Sullivan and Eric Burger, '"In the Public Interest": The Privacy Implications of International Business-to-Business Sharing of Cyber-Threat Intelligence' (2017) 33(1) *Computer Law & Security Review* 14; Adrian Haase and Emma Peters, 'Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance' (2017) 7(2) *International Data Privacy Law* 126; Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' (2018) 8(1) *International Data Privacy Law* 52.

[113] Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*, 844/14/EN, WP 217 (9 April 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[114] Emphasis added.

[115] Compare the judgment of the CJEU in Case C-175/20, *'SS' SIA* v. *Valsts ieņēmumu dienests* [2022] ECLI:EU:C:2022:124, confirming that tax authorities require a specific legislative measure compliant with Article 5(1) GDPR to demand information from an internet advertising site regarding customers.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

12.4.3.5 Is Voluntary Disclosure Permitted after the European Electronic Communications Code?

The European Electronic Communications Code (EECC)[116] should also be mentioned as restricting the situations where voluntary disclosure might be permitted. The EECC extends the protections of the ePrivacy Directive to over-the-top communications services that qualify as 'interpersonal communications services', including both number-based and number-independent services. For those providers, therefore, voluntary disclosure of information about user communications is likely to constitute a breach of their obligations under the Irish transposition of the confidentiality provisions of the ePrivacy Directive.[117]

12.4.3.6 Admissibility of Data Provided through Voluntary Cooperation

Turning to admissibility, all data obtained through voluntary cooperation is capable of being used in criminal proceedings, subject to the ordinary rules of evidence. Any voluntary disclosure of information can in principle be challenged by the individual whose data is sought (for example, on the grounds that disclosure violated the data protection obligations of the provider). As with mandatory cooperation, however, the practical ability to do so will depend on whether the individual is notified, and there is no obligation in Irish law for notification. The admissibility of evidence obtained in this way can also be challenged by a defendant in any subsequent criminal trial, and the exclusionary rule will mean that such evidence may be excluded if it was obtained illegally or unconstitutionally.

12.4.4 *Overview of Existing Cooperation Duties*

Irish law recognises a number of means of accessing data, as already discussed throughout this chapter. The appropriate method of access in a particular investigation will depend on the type of data required, the circumstances that require the data access and whether the relevant service provider meets the definition of 'authorised undertaking' or 'service provider' in the case of interception and data retention respectively. Table 12.1 summarises the main methods and their key features.

It may also be helpful at this point to identify areas where Irish law does *not* provide for mandatory cooperation with providers. There are no provisions in Irish criminal law for real-time collection or recording of traffic or content data (other than under the interception and data retention systems), or blocking access to or takedown of web pages.[118] Some providers may voluntarily agree to take on responsibilities – for example, some internet service providers

[116] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. The EECC was transposed into Irish law by the European Union (Electronic Communications Code) Regulations 2022 (SI No. 444 of 2022).

[117] Regulation 5 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI No. 36 of 2011) as applied by Regulation 112(1)(a) of the European Union (Electronic Communications Code) Regulations 2022 (SI No. 444 of 2022).

[118] There are some narrow exceptions. For example, in the case of internet gambling, section 32A of the Betting Act 1931, as amended by section 28 of the Betting (Amendment) Act 2015, makes it illegal to provide internet services to an unlicensed remote (online) bookmaker and authorises the Revenue Commissioners to issue an enforcement notice prohibiting such services. In relation to sanctions against Russia, the communications regulator ComReg has taken the view that Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, [2022] OJ L 65, 2 March 2022 requires Irish ISPs to block access to the Russia Today and Sputnik websites. As of January 2024, mandatory website blocking under the Terrorist Content Regulation, Regulation (EU) 2021/784 of the European

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

TABLE 12.1 *Summary of data access methods under Irish law*

Data access mechanism?	What type of data can be obtained?	Who can be targeted?	Legal basis and authorising body?	Grounds?
Search warrants	Any information already held by the provider (including content data); cannot require ongoing interception or generation of data. Whether passwords or decryption keys must be disclosed depends on the type of crime and the precise statutory power relied upon.	A search warrant can be issued in respect of any place in the state, including locations of telecoms providers; information society service providers generally; and over-the-top services.	Various statutory powers depending on the offence being investigated, e.g. section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 for most cybercrime offences. Court ordered.	Generally limited to investigation etc. of offences carrying a possible five-year prison sentence.
Production orders	Any information already held by the provider (including content data); cannot require ongoing interception or generation of data. Whether passwords or decryption keys must be disclosed depends on the type of crime and the precise statutory power relied upon.	Any natural or legal person in the state/carrying on business in the state can be issued with a production order, including: telecoms and connectivity providers; information society service providers generally; and over-the-top services.	Various statutory powers depending on the offence being investigated, e.g. section 15 of the Criminal Justice Act 2011. Court ordered.	Generally limited to investigation etc. of offences carrying a possible five-year prison sentence.
Interception warrants	Telecommunications messages (content); warrants may require interception on an ongoing basis or access to stored telecommunications messages.	Only 'authorised undertakings': essentially traditional telecoms and connectivity providers but not, e.g., over-the-top communication services, webmail providers or other information society services.	Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993. Requires a warrant signed by the Minister for Justice and Equality.	Investigation etc. of serious offences (defined as carrying a possible five-year prison sentence and meeting additional criteria such as loss of life, serious personal injury, substantial gain or other especially serious factors); security of the state.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

TABLE 12.1 *(continued)*

Data access mechanism?	What type of data can be obtained?	Who can be targeted?	Legal basis and authorising body?	Grounds?
Access to retained data	User data, internet source data, Schedule 2 data (location and communications traffic data).	Applies only to 'service providers': essentially traditional telecoms and connectivity providers but not, e.g., over-the-top communication services, webmail providers or other information society services.	Communications (Retention of Data) Act 2011. Requires internal authorisation within police and other investigative agencies (user data) or judicial authorisation (internet source data and Schedule 2 data). There are exceptions to the requirement of judicial authorisation in cases of urgency.	Varies according to the data sought. User data is available in relation to investigation etc. of criminal offences generally, as well as revenue offences; police disciplinary matters; the security of the state; the saving of human life; and locating a missing person. Internet source data is available in relation to investigation etc. of serious offences (carrying a possible five-year prison sentence); revenue offences; police disciplinary matters; the security of the state; the saving of human life; and locating a missing person. Schedule 2 data is generally available only in relation to state security, unless the data is being held for a purpose other than compliance with a High Court order imposing data retention obligations, in which case it is also available in relation to serious offences, revenue offences and police disciplinary matters.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

TABLE 12.1 *(continued)*

Data access mechanism?	What type of data can be obtained?	Who can be targeted?	Legal basis and authorising body?	Grounds?
Voluntary access to user data	Potentially any information, but, in practice, usually non-content data only.	Any data controller based in Ireland. This can include telecoms providers, information society service providers and over-the-top communication services.	Section 41 of the Data Protection Act 2018. (Previously section 8 of the Data Protection Acts 1988 and 2003.) No official authorisation is required by law; in practice, providers usually require sign-off by a senior official in the relevant agency.	Investigation etc. of offences, national security, defence and public security.

(ISPs) voluntarily block access to websites said to contain child abuse images[119] – but there is no legal framework around these areas. There is no provision in Irish law for data preservation (quick freeze) orders in support of criminal investigations, except in relation to those traditional telecommunications and connectivity providers such as mobile phone operators who are 'service providers' within the scope of the Communications (Retention of Data) Act 2011.[120]

12.4.4.1 Encryption

As discussed in Section 12.2.1, whether a statutory power requires disclosure of encryption keys or decrypted text depends on the exact power used. Production orders usually require information to be produced in a form in which it is 'visible and legible'.[121] For example, section 15(6) of the Criminal Justice Act 2011 provides that:

> Where the documents concerned are not in legible form, an order under this section shall have effect as an order—
>
> (a) to give to a member of the Garda Síochána any password necessary to make the documents legible and comprehensible,
> (b) otherwise to enable the member of the Garda Síochána to examine the documents in a form in which they are legible and comprehensible, or
> (c) to produce the documents to the member of the Garda Síochána in a form in which they can be removed and in which they are, or can be made, legible and comprehensible.

Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), [2021] OJ L 172, 17 May 2021, has not been implemented in Irish law.

[119] T. J. McIntyre, 'Cybercrime in Ireland: Towards a Research Agenda', in Deirdre Healy, Claire Hamilton, Yvonne Daly and Michelle Butler (eds.), *The Routledge Handbook of Irish Criminology* (Abingdon: Routledge, 2015), 110–111.

[120] Communications (Retention of Data) Act 2011, ss. 7A and 7B.

[121] See, e.g., Criminal Justice (Theft and Fraud Offences) Act 2001, s. 52.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

This means that, for example, a provider ordered to disclose data which it holds on behalf of a user will have to remove any encryption applied by the provider itself. However, it will not require decryption of data where the key is held by the user, or backdooring of systems such as end-to-end encryption.[122]

Some search warrants give police the power to require a person with access to a computer at the location being searched to provide relevant passwords and encryption keys that are necessary to render information visible and legible.[123] But note that these powers relate to individuals who are physically present at a particular place while it is being searched – they are not free-standing powers to demand passwords or encryption keys in other circumstances. There are no specific provisions to safeguard rights in the context of encrypted information, and decrypted data is admissible in criminal proceedings subject to the ordinary rules of evidence.

12.4.4.2 Law Enforcement Agency Hacking

Irish law does not specifically provide for state hacking.[124] It is possible that state malware could be used as a 'surveillance device' under the regime established by the Criminal Justice (Surveillance) Act 2009; however, there is no public information as to whether this has happened or whether Irish police have this capability.[125] It should be noted that the 2009 Act does not permit the use of surveillance devices in a way that would amount to an 'interception of communications' as defined by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, so that if state malware is deployed it would have to be tailored to avoid capturing phone calls, text messages and emails if they fall within the scope of the 1993 Act.[126]

12.4.4.3 Interception Capability Requirements

There is no general statutory power requiring providers to change the technical infrastructure or security settings of their services to make them vulnerable to interception. However, in relation to 'authorised undertakings' (traditional telecommunication providers), a government Minister may issue directions in writing, requiring them to do anything which the Minister may specify from time to time as necessary in the national interest.[127] These directions are kept secret, but appear to include requirements to build in intercept capability.[128]

[122] Given the principle that powers infringing on privacy must be strictly construed, and the practical and financial impact of requiring a provider to attempt to undermine user encryption or backdoor their system, this section must be read as only requiring disclosure of a password held by a provider rather than any more invasive actions. See, e.g., *Byrne* v. *Grey* [1988] IR 31.

[123] See, e.g., Criminal Justice (Offences Relating to Information Systems) Act 2017, s. 7(4).

[124] Without some statutory basis, state malware would most likely constitute the offence of accessing an information system without lawful authority contrary to section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017.

[125] The Irish authorities have stated that '[s]urveillance warrants can be obtained under the Criminal Justice (Surveillance) Act 2009 to monitor computers that use encryption, and this can overcome difficulties in serious criminal cases where it is known that encryption is being used and passwords will not be handed over'. It is not clear whether this refers to hacking, but the context suggests that it does. See, e.g., Council of the European Union, *Report on Ireland*, 68.

[126] Criminal Justice (Surveillance) Act 2009, s. 2(3).

[127] Section 110 of the Postal and Telecommunications Services Act 1983 (as amended). There is an obvious question mark as to whether such a wide power, exercised in secret, is a sufficient legal basis for the purposes of Article 8 ECHR.

[128] In 2016 a ministerial answer to a parliamentary question stated: 'Telecommunications services providers are required to maintain a capacity to intercept telecommunications messages in accordance with the provisions of section 110 of

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

12.4.4.4 Territorial Scope

The number of providers with a presence in Ireland but operations elsewhere means that the territorial scope of domestic powers is of crucial importance. In addition to determining which providers come within the scope of these powers, we must also determine whether it is possible to compel those providers to disclose data hosted outside the state. To put it another way: does Irish law permit any extraterritorial jurisdiction similar to that asserted by the United States in the *Microsoft Ireland* litigation? The answer will depend in each case on the nature of the power being used.

12.4.4.5 Search Warrants

Search warrants are inherently territorial and so can only be granted in respect of premises located within the state (the location of the individual whose data is sought is irrelevant). Some search warrants, however, appear to permit access to data held on computers outside the state where it is accessible by means of a computer at the place being searched. Consider, for example, section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017. Search warrants under this section permit a member of An Garda Síochána to 'operate any computer at the place that is being searched'.[129] However, the section defines 'computer at the place that is being searched' to include 'any other computer, *whether at the place being searched or at any other place*, which is lawfully accessible by means of that computer'.[130] On the face of it, this permits 'remote searches' or 'network searches', including searches of computers located in other jurisdictions. It would, for example, seem to permit access to webmail hosted abroad where a device at the place being searched is logged in to that service. This presents difficult comity issues, particularly where such searches would not be permitted in those other jurisdictions, and it is surprising that the legislative history for this section does not address this point.[131]

12.4.4.6 Production Orders

A similar point arises in respect of production orders, which are territorial in the sense that they are available against any person in the state[132] who has 'possession or control' of documents but do not necessarily require that the *documents* must also be located within the state.[133] For example, under section 15(18) of the Criminal Justice Act 2011, a District Court judge has jurisdiction to make a production order if a company carries on business in the relevant district, whether or not the documents are also located in that district.[134]

the Postal and Telecommunications Services Act 1983, as amended. The State does not reimburse the costs associated with this.' Frances Fitzgerald, Written Answers, Dáil Éireann, 16 September 2016, 171.

[129] Criminal Justice (Offences Relating to Information Systems) Act 2017, s. 7(4)(a).

[130] Criminal Justice Act 2017, s. 7(9). Emphasis added.

[131] For background on remote searches. See, e.g., Susan Brenner, 'Law, Dissonance, and Remote Computer Searches' (2012) 14(1) *North Carolina Journal of Law & Technology* 43; Bert-Jaap Koops and Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* (Tilburg: TILT, 2014), https://repository.wodc.nl/bitstream/handle/20.500.12832/2047/2326-volledige-tekst_tcm28-73009.pdf?sequence=2&isAllowed=y.

[132] These powers generally apply to a person 'carrying on business in the state' also. There is no case law as to whether 'carrying on business in the state' would include providers who serve Irish customers but who do not have any physical presence in the state.

[133] The location of the individual whose data is being sought is also irrelevant.

[134] Criminal Justice Act 2011, s. 15(18), emphasis added. Section 52 of the Criminal Justice (Theft and Fraud Offences) Act 2001 creates a similar power with the same uncertainty as to its scope.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

The better argument is probably that these production order powers are implicitly limited to documents within the state[135] – under section 15(5) of the Criminal Justice Act 2011, for example, it is possible to grant an order for entry to the place where documents are kept, which would be inappropriate in relation to documents held in another state – but this and similar statutory powers are not clear on this point. There is no case law directly on this issue, but in *Walsh* v. *National Irish Bank*[136] the Supreme Court held that an equivalent revenue law power could be used to order disclosure of documents held by a foreign branch of an Irish bank, unless to do so would put the bank in breach of foreign law.

It may be that discussion of the extraterritorial scope of search warrants and production orders is moot. In the 2017 European Council Mutual Evaluation on Combating Cybercrime, the Irish authorities summarised their understanding of Irish law as being that providers can only be obliged to produce evidence 'located in Ireland'.[137] It seems unlikely that they will subsequently take a different interpretation – given the importance of the internet industry in Ireland there would be political costs in doing so, and by opting in to the e-Evidence proposals, Ireland will in any event benefit from extraterritorial jurisdiction. Nevertheless, the lack of certainty on this point is undesirable.

12.4.4.7 Interception of Communications and Data Retention

The interception and data retention powers apply to 'authorised undertakings' and 'service providers'.[138] As already discussed, these terms are defined in accordance with the EU telecommunications framework.[139] The legislation does not address the question of territorial scope, but in principle any such provider who is providing a service in Ireland would appear to be within the scope of these powers, regardless of the location of the headquarters or data storage. The legislation does not make these powers contingent on the location of the individual, and in principle these powers can be exercised in respect of an individual located abroad. Where an interception of communications is carried out in relation to an individual elsewhere in the EU then the other member state must be notified in accordance with the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[140] There is no similar requirement in relation to access to retained data.

12.4.5 *Legal Remedies and Protection of Fundamental Rights*

Irish law has long failed to provide adequate fundamental rights safeguards around state surveillance; instead, the state has adopted a reactive approach where reform has been a grudging and minimal response to scandal and litigation.[141] A full account of the fundamental rights issues around access to data processed by providers is beyond the scope of this chapter, but a number of aspects should be highlighted.

[135] Compare *Chemical Bank* v. *McCormack* [1983] ILRM 350 and *Walsh* v. *National Irish Bank* [2007] IEHC 325, discussed in Law Reform Commission, *Report on Search Warrants and Bench Warrants*.

[136] *Walsh* v. *National Irish Bank* [2013] IESC 2.

[137] Council of the European Union, *Report on Ireland*, 109.

[138] Communications (Retention of Data) Act 2011; Regulations 2003 (SI 306 of 2003).

[139] Regulations 2003 (SI 306 of 2003), regulation 4.

[140] Criminal Justice (Mutual Assistance) Act 2008, s. 26.

[141] T. J. McIntyre, 'Implementing Information Privacy Rights in Ireland', in Suzanne Egan (ed.), *Implementing Human Rights in Ireland* (Dublin: Bloomsbury Academic, 2015), 271–287; Maria Helen Murphy, 'The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases' (2013) 3(2) *Irish Journal of Legal Studies* 65; Maria Helen Murphy, 'Surveillance and the Right to Privacy: Is an "Effective Remedy" Possible?', in Alice Diver and Jacinta Miller (eds.), *Justiciability of Human Rights Law in Domestic Jurisdictions* (Heidelberg: Springer, 2015), 289–306.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

12.4.5.1 Notification

There is no provision in Irish law requiring that individuals be notified of the fact that their data has been accessed (except where Schedule 2 data is accessed under the Communications (Retention of Data) Act 2011). This is the case regardless of whether the individual is a suspect or notification would present a risk to an ongoing investigation. As already mentioned, some of the major US providers such as Apple, Facebook, Microsoft and Yahoo do commit to notifying users where their personal information is sought (subject to limitations), but this is purely a matter of policy on their part.[142]

12.4.5.2 Redress

In relation to interception and data retention, there is a statutory complaints mechanism that permits an individual to apply to a 'Complaints Referee' (usually a sitting Circuit Court judge) to investigate whether a ministerial authorisation for interception or a disclosure requirement for data was made and, if so, whether the requirements of the relevant act were followed in respect of the request.[143] This is an inquisitorial procedure: the Referee has the power to access any official documents relating to the measure. If the Referee concludes that the law has been contravened, they must notify the applicant in writing of that conclusion and make a report of their findings to the Taoiseach (Prime Minister). The Referee may also, if they think fit, quash the ministerial authorisation, direct the relevant agency to destroy the information obtained and recommend the payment of compensation to the complainant.

This redress system is, however, very limited. It is essentially limited to investigating whether a ministerial warrant or disclosure requirement was issued properly – it does not provide a remedy in relation to other situations such as improper retention or disclosure by the telecommunications provider, or misuse of data by police. The remedies are discretionary rather than a matter of right – in each case the destruction of the information obtained and the award of compensation are only if the Complaints Referee 'thinks fit'. There is almost no transparency regarding the activities of the Complaints Referee; investigations and decisions are not publicised and the Irish government has stated that it does not hold records on the number of complaints received or any details of such complaints.[144] However, it seems that there has never been a successful complaint to the Complaints Referee.[145]

12.4.5.3 Oversight

In relation to interception of communications and data retention, there is judicial oversight by a 'designated judge' (a sitting judge of the High Court) who has the duty of keeping the operation of the legislation under review and publishing annual reports.[146] In practice, this consists of yearly meetings with officials from the Department of Justice, the police and other agencies who use interception and data retention powers, and some inspection of their files.

[142] The T-CY Cloud Evidence Group, *Criminal Justice Access to Data in the Cloud*, s. 2.2.5.

[143] Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, s. 9; Communications (Retention of Data) Act 2011, s. 10.

[144] Dan MacGuill, 'State Surveillance: How Gardaí and Others Can Secretly Monitor You', *Journal*, 17 May 2015, www.thejournal.ie/state-surveillance-ireland-gardai-wiretapping-email-monitoring-gardai-2099537-May2015/.

[145] See, e.g., the answer of the Minister for Justice, Equality and Law Reform to a parliamentary question on this point. Brian Lenihan, Written Answers, Dáil Éireann, 4 March 2008, 111, 148, 501 and 502.

[146] Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, s. 8; Communications (Retention of Data) Act 2011, s. 11.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

However, the effectiveness of this process, like the Complaints Referee procedure, has been strongly criticised.[147] The oversight role is a part-time function of a judge with a full judicial caseload. The role has no staff and no specialist legal or technical support, meaning that there is no institutional memory and making it dependent on the entities being monitored. Until quite recently the annual reports almost always consisted of one or two pages with a few formulaic paragraphs reciting that, on a particular day, certain (unspecified) documents were inspected, certain (unspecified) queries were answered and, as a result, the judge was satisfied that the relevant authorities were in compliance with the law.[148]

One recently appointed designated judge took some steps to address these criticisms. In her 2018 annual report, Baker J. provides slightly more detail on the operation of these systems.[149] However, that report still came to a total of only four pages and illustrates weaknesses in the oversight system. Although Baker J. identified the data retention system as contrary to European fundamental rights standards following *Tele2*, she lacked the power to require that it be suspended until a proper legal basis was established and no action was taken on the basis of her report.

12.4.5.4 Failings in the Current Legal Framework

It is clear that significant reform of Irish law on access to data is required to achieve even bare compliance with ECHR and Charter of Fundamental Rights requirements.[150] A full account of these European norms and the deficiencies of the existing legal framework is beyond the scope of this chapter, but, drawing on the discussion earlier in the chapter, we can briefly summarise the main areas where reform is needed.

The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 fails to provide sufficient safeguards for data subjects. Notably absent from the regime are a requirement for judicial authorisation, procedures for notification where notification would not be prejudicial to an investigation, an effective oversight process and transparent procedures allowing for adequate redress. In addition, the 1993 Act permits interception of journalists' communications without prior judicial authorisation, contrary to the standards established by the ECtHR in *Telegraaf Media* v. *the Netherlands*,[151] and similarly fails to protect lawyer–client privileged communications.

The Communications (Retention of Data) Act 2011 still fails to address the majority of the issues identified in the Murray report, notwithstanding the changes made by the Communications (Retention of Data) (Amendment) Act 2022. The definition of 'serious offence' is excessively broad and permits disproportionate access to personal data. There is no definition of the national security purposes that justify access to data. As with interception, there are no

[147] T. J. McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective', in Martin Scheinin, Helle Krunke and Marina Aksenova (eds.), *Judges as Guardians of Constitutionalism and Human Rights* (Cheltenham: Edward Elgar, 2016).

[148] The annual reports of the designated judge and other official materials are available at Digital Rights Ireland, 'Surveillance Library', https://web.archive.org/web/20220120104440/https://www.digitalrights.ie/irish-surveillance-documents/.

[149] Marie Baker, *Report of Designated Judge Made Pursuant to Section 8(2) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and Section 12(1)(c) of the Communications (Retention of Data) Act 2011* (Houses of the Oireachtas, 28 June 2018), http://opac.oireachtas.ie/AWData/Library3/TAOdoclaid02082018d_113723.pdf.

[150] McIntyre, 'Judicial Oversight of Surveillance'; Murphy, 'Surveillance and the Right to Privacy'.

[151] *Telegraaf Media* v. *The Netherlands*, Appl. No. 39315/06, 22 November 2012.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

protections in place in relation to journalists' sources. The 2011 Act also fails to provide a cause of action for wrongful access to data.

The reliance by Irish police on voluntary disclosure by providers is also problematic. The intrusiveness of this practice is mitigated somewhat by the fact that the most important providers provide only non-content data in this way, but it is astonishing that stored over-the-top communications, subscriber information and communications metadata can be provided without any clear legal basis, prior judicial approval, notification, subsequent judicial oversight or redress mechanism. In permitting access to the *content* of communications in this way, Ireland fails to meet the requirements of ECHR case law from *Klass* v. *Germany* onwards, which requires that at a minimum there must be oversight mechanisms established by law that are 'independent of the authorities carrying out the surveillance', 'objective' and 'vested with sufficient powers and competence to exercise an effective and continuous control' over communications surveillance.[152]

Even in relation to *non-content data*, this voluntary disclosure is of very dubious legality. In relation to subscriber data, for example, there is considerable authority that identifies the sensitivity of this data as requiring a statutory basis for disclosure. In *R* v. *Spencer*,[153] the Canadian Supreme Court held that a police request for voluntary disclosure of subscriber information from an ISP was a search that violated section 8 of the Canadian Charter of Rights. This was notwithstanding a provision in the Personal Information Protection and Electronic Documents Act (PIPEDA) which permitted disclosure where a law enforcement agency had requested personal information and had 'lawful authority' to do so; the Supreme Court took the view that 'lawful authority' in this context meant a compulsory power to require disclosure, not merely a power to ask. The 2018 ECtHR judgment in *Benedik* v. *Slovenia*[154] reaches a very similar result in holding that Slovenia violated Article 8 ECHR by failing to provide an adequate legal framework around access to ISP subscriber information. In light of these precedents, Irish practice is on shaky ground.

In addition to changes to the rules regarding access to data, it will be important to introduce an effective institutional framework to ensure that those rules are followed. The EU Fundamental Rights Agency has recommended in relation to state surveillance that

> [t]he independence of oversight bodies should be enshrined in law and applied in practice. EU Member States should grant oversight bodies adequate financial and human resources, including diverse and technically-qualified professionals. Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate. Member States should ensure that the oversight bodies' decisions are binding.[155]

In line with this recommendation, the designated judge role should be replaced by an oversight body, chaired by a judge with support from legal and technical specialists, with binding powers to order the cessation of surveillance activities. At the time of writing (February 2024) there is some reform taking place: the role of the designated judge is in the process of being transferred to a newly established Independent Examiner of Security Legislation under the Policing, Security

[152] *Klass* v. *Germany*, Appl. No. 5029/71, 6 September 1978, para. 56.
[153] *R.* v. *Spencer*, 2014 SCC 43, [2014] 2 SCR 212.
[154] *Benedik* v. *Slovenia*, Appl. No. 62357/14, 24 April 2018.
[155] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Field Perspectives and Legal Update*, 2 vols. (Luxembourg: Publications Office of the European Union, 2017), vol. II, p. 11, https://publications.europa.eu/en/publication-detail/-/publication/b7f98a74-afc2-11e7-837e-01aa75ed71a1/language-en.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

and Community Safety Act 2024. This, however, is largely a change of personnel rather than function – the new Independent Examiner will have the same limited role and powers as the designated judge – and is not enough to ensure adequate oversight.

12.5 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

12.5.1 *Introduction*

Despite the growing importance of Ireland as a centre for internet firms, there is little domestic law on the issue of cross-border cooperation in relation to access to data held by providers. The following subsections outline the current state of play on important matters, including the potential ratification of the Cybercrime Convention.

12.5.1.1 Convention on Cybercrime

Ireland signed the Cybercrime Convention on 28 February 2002 but has yet to ratify it.[156] Until 2017, domestic law failed to address either the substantive offences or the procedural provisions required by the Convention. In 2017, the substantive offences were finally transposed into Irish law, but there is still no legislation in place dealing with the procedural provisions, such as expedited preservation of data.[157]

12.5.1.2 European Investigation Order

Ireland chose not to opt into the draft EIO Directive when it was proposed in 2010. In 2014, the then Minister for Justice and Equality, Frances Fitzgerald, explained that this was on the basis that the draft directive was 'inconsistent with Irish law and practice', in particular owing to the limited grounds for non-recognition and non-execution of an EIO and the lack of a general dual criminality requirement.[158] The Minister indicated that Ireland would consider opting in to the EIO, but as of December 2022 this has not happened.

12.5.1.3 MLA Agreements and Criminal Justice (Mutual Assistance) Act 2008

In the absence of powers under the Cybercrime Convention or the EIO Directive, the primary legal basis for cross-border cooperation are the mutual legal assistance (MLA) agreements to which Ireland is a party. These are given legal effect by the Criminal Justice (Mutual Assistance) Act 2008, which designates the Minister for Justice and Equality as the Central Authority for the purposes of dealing with requests.[159]

Ireland does not publish statistics on the number of MLA requests made to or by the Irish authorities. However, a 2017 evaluation of Irish practice regarding cybercrime provides

[156] For background, see, e.g., McIntyre, 'Cybercrime in Ireland'.
[157] The offences were transposed by the Criminal Justice Act 2017. There is limited provision for preservation of some communications data under the Communications (Retention of Data) Act 2011.
[158] Frances Fitzgerald, Written Answers, Dáil Éireann, 4 June 2014, 164–166.
[159] See, e.g., Department of Justice and Equality, *Mutual Legal Assistance in Criminal Matters: A Guide to Irish Law and Procedures* (July 2008).

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

a snapshot: in 2015 the central authority received 615 incoming MLA requests (of which approximately 160 were for material stored by providers in Ireland) and 250 outgoing requests.[160] Seventy-seven of these outgoing requests were to the United States, and these were described as 'primarily' for material stored by providers.[161] It should be noted that these figures significantly understate the extent to which there is international cooperation in this area – because they are limited to cases where the MLA procedure is used, they will not capture situations where firms with an Irish presence respond to overseas requests on a voluntary basis. Similarly, these statistics may not fully reflect the extent to which Irish authorities rely on material from the large providers; for example, requests to Facebook (for non-content data) may have been made under domestic law to Facebook Ireland Ltd rather than through the MLA process.[162]

12.5.1.4 Data Localisation

Irish law does not have any distinct data localisation rules for providers. The only applicable rules are the ordinary rules of EU data protection law prohibiting transfer to third countries.

12.5.2 *Cooperation of National LEAs with Foreign Service Providers (Outbound Requests from Ireland): Legal Framework and Nature of the Cooperation*

12.5.2.1 Access to Data

The Criminal Justice (Mutual Assistance) Act 2008 provides the legal framework for access by Irish police to data held by foreign providers. In general, it applies to 'designated states' – defined as EU member states and other states designated by the Minister for Foreign Affairs.[163]

The most important provisions are sections 62 and 73, which provide for taking evidence from a person in a designated state and searching for evidence at a place in a designated state. In any criminal investigations or criminal proceedings, the Director of Public Prosecutions or a judge may send a letter of request to the Central Authority specifying the evidence which is sought and including:

- a statement that the evidence is required for the purpose of criminal proceedings or a criminal investigation,
- a brief description of the conduct constituting the offence concerned and
- any other available information that may assist the appropriate authority in complying with the request.

When evidence is obtained under these sections, its use is restricted. The evidence may not be used for any purpose other than that permitted by the relevant international instrument or specified in the letter of request without the consent of the appropriate authority in the designated state. When the evidence is no longer required for that purpose (or for any other purpose for which such consent has been obtained), it must be returned to the appropriate

[160] Council of the European Union, *Report on Ireland*, 103.
[161] Ibid.
[162] See, e.g., Data Protection Commissioner, *Facebook Ireland Report of Audit*, 99.
[163] Criminal Justice (Mutual Assistance) Act 2008, s. 4.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

authority unless the authority indicates that it need not be returned. Both sections 62 and 73 also provide for this evidence to be admissible without further proof.

12.5.2.2 Interception of communications

Requests for interception of communications are regulated by part 3 of the Criminal Justice (Mutual Assistance) Act 2008, which gives effect to Articles 17 to 22 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union 2000. Section 23 deals with the situation where technical assistance is needed from a member state,[164] and provides that the Minister for Justice may request a competent authority in another member state to carry out interception for transmission to the Garda Síochána. Section 26 addresses the situation where a telecommunications address is being used in another member state and technical assistance is not required for an interception to be carried out, and provides for notification by the Minister of the competent authority in the relevant state.

In each case, however, these provisions apply only where the Minister has given an authorisation for an interception under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993. As already discussed, that legislation applies only to messages being transmitted by 'authorised undertakings' and therefore does not apply to over-the-top communication services, which fall outside the scope of the telecommunications law framework.[165]

The result is a significant gap in that the Criminal Justice (Mutual Assistance) Act 2008 does not permit the Minister to seek interception of communications on over-the-top services in other member states – even where the domestic law of those member states does provide for such interception.[166]

12.5.2.3 Legal Remedies and Protection of Human Rights

Section 107 of the Criminal Justice (Mutual Assistance) Act 2008 enforces any restrictions in MLA treaties on the use of personal data obtained from another jurisdiction by providing that the 'provisions of the relevant international instrument have effect in respect of the use of personal data communicated to or otherwise obtained by a person in the State under the instrument'. It also confirms that data protection law applies in respect of the data. The 2008 Act otherwise does not create any additional legal remedies or specific fundamental rights safeguards regarding to access to data held outside Ireland or interception of communications outside Ireland.

12.5.2.4 Irish Views on the Effectiveness of the MLA Process

In the 2017 European Council Mutual Evaluation on Combating Cybercrime, the Irish authorities 'stressed the fact that the MLA process is time-consuming and the processes can be cumbersome'.[167] This reflects a general view within Irish police; for example, one garda (police

[164] Defined in section 2 of the Criminal Justice (Mutual Assistance) Act 2008 to mean other EU member states, plus Iceland and Norway and any other state which might be designated under section 4. No other states have been yet designated for the purpose of part 3 of the Act on interception of communications.

[165] Denis Kelleher, *Privacy and Data Protection Law in Ireland* (Dublin: Tottel, 2006), 454.

[166] Access to stored communications would still be possible through a request under section 62 or section 73 of the Criminal Justice (Mutual Assistance) Act 2008; however, requests for real-time interception would be precluded.

[167] Council of the European Union, *Report on Ireland*, 109.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

officer) was quoted anonymously in the media as saying that social media investigations are significantly hampered by the delay in receiving responses to MLA requests.[168]

12.5.3 *Cooperation of National Service Providers with Foreign LEAs (Inbound Requests to Ireland)*

12.5.3.1 Mandatory Cooperation

The Criminal Justice (Mutual Assistance) Act 2008 requires Irish providers to provide information to foreign law enforcement agencies in response to an MLA request. The key provisions are sections 24 and 25, dealing with incoming requests for interception of telecommunications messages, and sections 63, 74 and 75 on the taking of evidence and searches for evidence.

12.5.3.2 Taking Evidence: Questioning Witnesses

Section 63 of the Criminal Justice (Mutual Assistance) Act 2008 deals with inbound requests for evidence to be taken from a witness, for the purpose of criminal proceedings or a criminal investigation in a designated state. Taking evidence in this context primarily means questioning witnesses, but may also involve a witness being compelled to produce a document.

On receiving such a request, the Minister for Justice and Equality may[169] request the President of the District Court to nominate a judge to receive the evidence; doing this confers on that judge the powers of the District Court in criminal proceedings, including the power to compel witnesses and to secure the production of documents.[170] Failure to give evidence or to produce a document, without reasonable excuse, is an offence carrying a possible fine of €2,500 or imprisonment for up to six months. There is no requirement of dual criminality in relation to this power. Witnesses may assert any applicable privilege which would apply in criminal proceedings either in Ireland or in the state seeking the evidence.[171]

12.5.3.3 Access to Data

Sections 74 and 75 of the Criminal Justice (Mutual Assistance) Act 2008 deal with inbound requests for searches for evidence for use outside Ireland. Of these, section 75 is most relevant for the majority of cases involving access to data.

[168] Cathal McMahon, 'Gardaí Dealing with Avalanche of Social Media Complaints Claim "Unnecessary Obstacles" Put in the Way by Management and Web Firms', *Independent*, 29 April 2017, www.independent.ie/irish-news/news/garda-dealing-with-avalanche-of-social-media-complaints-claim-unnecessary-obstacles-put-in-the-way-by-management-and-web-firms-35664310.html.

[169] The power is a discretionary one. In *Agrama* v. *Minister for Justice, Equality and Law Reform* [2015] IESC 94, O'Donnell J. noted, regarding the precursor provision to section 63 of the 2008 Act:

> Having regard to the objective of mutual assistance, it will be only on rare occasions that the Minister would refuse. Refusal would normally require compelling reasons. It is not possible or desirable to provide an exhaustive list of the circumstances which would justify refusal. Such circumstances must be considered by reference to the facts of the individual case, but grounds which might amount to compelling reasons justifying refusal may be considerations such as national security, breach of a fundamental principle of justice, or abuse of the process. (para. 35)

Note that under section 3 of the Criminal Justice (Mutual Assistance) Act 2008 certain threats to fundamental rights will *require* that assistance be refused.

[170] Criminal Justice (Mutual Assistance) Act 2008, s. 63(4).

[171] Ibid., s. 64.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

The criteria for section 75 to apply are as follows:

- There must be a request from a designated state or a member state for evidential material.[172]
- The request must be for the purpose of criminal proceedings or a criminal investigation.[173]
- The alleged conduct would create a power under Irish law to issue a search warrant.[174]
- In the case of a request from a member state:
  - the conduct must be punishable by both Irish law and the law of the requesting state by 6 months' imprisonment; or
  - the conduct must be punishable by Irish law by 6 months' imprisonment and must be an infringement of the rules of law of the requesting state, being prosecuted by the administrative authorities, where the decision may give rise to proceedings before a court having jurisdiction in criminal matters;[175]
- In the case of a request from a designated state (other than a member state) the conduct in question must meet the standard of dual criminality.[176]

Where these criteria apply, the Minister for Justice and Equality may send the request to the Commissioner of the Garda Síochána to be complied with. If the Garda Síochána already has possession of the relevant material (for example, if a parallel domestic investigation is underway), it may be supplied in response to the request; otherwise, a member of the Garda of at least inspector rank shall apply to a District Court judge for an order in relation to the material[177] and that order may be granted if the judge is satisfied that there are reasonable grounds for believing that the person named in the order possesses the evidential material.[178]

The order which may be granted under section 75(10) of the Criminal Justice (Mutual Assistance) Act 2008 is effectively a hybrid production order and search warrant, requiring production of the specified evidential material or giving access to it, and granting a member of the Garda Síochána power to enter and search the relevant place for the material, if necessary. It is a crime to obstruct a member of the Garda Síochána acting under an order, or to fail to comply with a requirement in the order.[179]

There is limited provision for decryption under section 75(11), which requires data to be provided in plaintext but will not require decryption of data where the key is held by the user, or backdooring of systems such as end-to-end encryption.[180] It should also be noted that, unlike some other statutory powers, this provision does not give police power to demand disclosure of a password or encryption key for the requested data; they are empowered to demand disclosure of merely the data itself in decrypted form.[181]

12.5.3.4 Interception of Communications

Inbound requests to the Irish authorities for interception of communications are regulated by sections 24 and 25 of the Criminal Justice (Mutual Assistance) Act 2008. Section 24 provides that

[172] Ibid., s. 75(1).
[173] Ibid.
[174] Ibid.
[175] Ibid., s. 74(2).
[176] Ibid., s. 75(3).
[177] Ibid., s. 75(8).
[178] Ibid., s. 5(9).
[179] Ibid., s. 75(16).
[180] See the discussion of similar statutory wording in Section 12.4.4 of this chapter.
[181] Unless the password or encryption key is itself the requested evidence.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

member states may request the Irish state to carry out interceptions for the purpose of criminal investigations if a lawful interception order has been issued in that member state. This covers two situations: where the person against whom the order applies is in Ireland, and where the person is in another member state but technical assistance from the Irish state is needed to intercept the messages. Requests are to be made by a competent authority in the requesting member state to the Minister for Justice.

Section 25 then sets out the basis on which the Minister may authorise the interception. To summarise:

- Where the person is outside Ireland, the Minister may authorise the interception if the requirements of section 24 are met (with no requirement of dual criminality or that the conduct would be a serious offence under Irish law).[182]
- Where the person is in Ireland then a higher standard applies: the Minister may authorise the interception if:
    - the requirements of section 24 are met; and
    - the conduct would also constitute a serious offence in Irish law and would justify the giving of a ministerial authorisation under domestic law.[183]
- Where the person is in Ireland, the Minister also may make the authorisation and use of the intercepted messages subject to any condition that would apply if the authorisation had been granted in a domestic context.[184]

These authorisations are deemed to be authorisations under the Interception of Postal Packets and Telecommunications (Regulation) Act 1993 – that is to say, this type of interception is an application of the domestic interception regime rather than an entirely new power.[185] This has two significant consequences. First, the limitations of the existing domestic regime apply in the context of interception on foot of a request from another member state. This means that interception under the Criminal Justice (Mutual Assistance) Act 2008 is not available in respect of any providers other than 'authorised undertakings', excluding over-the-top communications services.[186] Second, these interceptions also come within the scope of the Complaints Referee and designated judge oversight mechanisms under the 1993 Act.

12.5.3.5 Legal Remedies and Protection of Fundamental Rights

12.5.3.5.1 REFUSAL OF ASSISTANCE. Section 3(1)(b) of the Criminal Justice (Mutual Assistance) Act 2008 provides that requests for assistance under the Act shall be refused if

> there are reasonable grounds for believing
>
> (i) that the request concerned was made for the purpose of prosecuting or punishing a person on account of his or her sex, race, religion, ethnic origin, nationality, language, political opinion or sexual orientation, [or]
> (ii) that providing assistance—

[182] Criminal Justice (Mutual Assistance) Act 2008, ss. 25(1) and 25(2). Note that requests for immediate transmission are preferred, so requests for interception and recording followed by transmission of the recording can be authorised only if immediate transmission is not possible: s. 25(2).
[183] Ibid., s. 25(3).
[184] Ibid., s. 25(5).
[185] Ibid., s. 25(8).
[186] Council of the European Union, *Report on Ireland*, 104.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

(I) may prejudice a person's position for any of those reasons, or
(II) may result in the person being subjected to torture or to any other contravention of the European Convention on Human Rights.

12.5.3.5.2 PURPOSE LIMITATION. There is a purpose limitation principle in the case of each of the statutory powers[187] to take evidence and search for data in response to inbound requests: an assurance must be given by the requesting authority (a) that any evidence supplied in response to the request will not, without the Minister's prior consent, be used for any purpose other than that permitted by the relevant international instrument or specified in the request, and (b) that the evidence will be returned when no longer required for that purpose[188] unless the Minister indicates that its return is not required.[189]

12.5.3.5.3 NOTIFICATION. There is no statutory provision for notification of individuals that their data is to be accessed (or has been accessed) under mutual assistance procedures. This has been unsuccessfully challenged on fair procedure grounds in the past; in *Brady* v. *Haughton*,[190] the Supreme Court considered the power to take evidence for mutual assistance under section 51 of the Criminal Justice Act 1994[191] and held that it was not unconstitutional by permitting evidence to be taken without notice to a party who may be affected. Instead, the majority in the Supreme Court described the procedure as an evidence-gathering exercise that would not give rise to an entitlement to be informed under domestic law.[192]

Whether or not there is notification will, therefore, depend on the policy of the provider. A problem in this regard is that section 100 of the Criminal Justice (Mutual Assistance) Act 2008 creates a very wide 'tipping-off' offence carrying a possible penalty of five years' imprisonment: 'Where a request[193] is made in connection with a criminal investigation in the State or a designated state, any person who, knowing or suspecting that the investigation is taking place, makes any disclosure which is likely to prejudice the investigation is guilty of an offence.' This offence does not require any intention to prejudice the investigation, merely knowledge or suspicion that an investigation is taking place. It is a defence for the defendant to prove that they '(a) did not know or suspect that the disclosure to which the proceedings relate was likely to prejudice the investigation concerned, or (b) had lawful authority or reasonable excuse for making the disclosure'. The term 'reasonable excuse' is not defined in the legislation, making it difficult for a provider to know whether it would be committing an offence by notifying a user of a mutual assistance request in accordance with its general policy.

[187] Criminal Justice (Mutual Assistance) Act 2008, ss. 63, 74 and 75.
[188] Or any other purpose for which such consent has been given.
[189] In the context of e-evidence, the obligation to return makes less sense but might be interpreted as an obligation to delete the local copy.
[190] *Brady* v. *Haughton* [2006] 1 IR 1.
[191] The precursor to section 63 of the Criminal Justice (Mutual Assistance) Act 2008.
[192] The position may be different in relation to particularly sensitive types of information: in *Brady* v. *Haughton* itself, a number of the judges expressed concern about access to medical records without notice, and in *Burns* v. *O'Neill* [2015] IEHC 553, *LK* v. *Minister for Justice and Equality* [2016] IECA 361 and *LK* v. *Minister for Justice and Equality* [2016] IECA 362, the state accepted that it was obliged to notify individuals where their medical records were sought. It is arguable that the same principle should apply in respect of telecommunications records; for the time being, however, there is no notification in this context.
[193] Defined as 'a request for assistance which is made by a requesting authority under and in accordance with a relevant international instrument'. Criminal Justice (Mutual Assistance) Act 2008, s. 2.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

12.5.3.5.4 DUTY OF DISTRICT COURT JUDGE TO CONSIDER PRIVACY RIGHTS. The privacy rights of an individual when evidence is sought for mutual assistance have been considered in *LK* v. *Minister for Justice and Equality*.[194] That case involved a letter of request from the UK for medical records concerning LK, who was to be a witness in a murder trial; the records were sought by the defendant with a view to discrediting her testimony. Her treating doctor and representatives from a hospital and another medical body were summoned to appear before a nominated District Court judge with the relevant records. Having been told that LK was vehemently opposed to the release of her information, each of them was legally represented and asserted, on her behalf, that the records were not compellable. This argument was rejected by the judge who found that production of the records could be compelled, notwithstanding that this form of third-party discovery would not be available in a domestic criminal matter.

Subsequently, LK brought a judicial review of that decision, and the Court of Appeal quashed the order to produce the evidence on the basis that the judge had erred by failing to consider her privacy rights under the Constitution and under Article 8 ECHR. *Per* Edwards J., where a District Court judge is nominated to take evidence relating to an individual, they are under an obligation 'to have regard to, and to take into account, the [individual's privacy rights] even if they had not been expressly asserted either by the [individual] or by an advocate putting forward a case on [their] behalf',[195] and in doing so must balance the rights of the individual against other considerations 'such as the public interest and the exigencies of the common good, and indeed the right of the defendant in the requesting state to receive a fair trial'.[196]

12.5.3.5.5 VOLUNTARY COOPERATION. We have already seen (in Section 12.4.3) how providers in Ireland developed a practice of voluntary disclosure of user data to police,[197] relying on section 8 of the Data Protection Acts 1988 and 2003. This extends to requests from law enforcement agencies in other jurisdictions – making Ireland, according to the Commission, the only jurisdiction in the EU to permit this.[198]

What is, perhaps, most striking about the cross-border nature of this practice is how little attention it has received. What is the legal basis for the provider to make voluntary disclosure to foreign law enforcement – particularly where the transfer is outside the EEA and bypasses the safeguards established by the existing mutual legal assistance framework?

There is almost no public information about this, apart from what emerged during Facebook's 2011 audit by the Data Protection Commissioner. During that audit Facebook argued that international disclosure of non-content data – worldwide, not just within the EEA – was permissible on the basis that either:

- the exception in section 8(b) of the Data Protection Acts 1988 and 2003 for 'preventing, detecting or investigating offences, apprehending or prosecuting offenders' permitted disclosure for foreign criminal investigations; or
- users consented to such disclosure through the Privacy Policy; or

[194] See *LK* v. *Minister for Justice and Equality* [2016] IECA 361 and [2016] IECA 362. While this case deals with section 63 of the Criminal Justice (Mutual Assistance) Act 2008 regarding the taking of evidence before a court, the same principles should apply regarding searches for evidence under sections 74 and 75 so that an order under those sections could also be quashed if it failed to take into account the privacy interests involved.

[195] See *LK* v. *Minister for Justice and Equality* [2016] IECA 362, para. 23.

[196] See *LK* v. *Minister for Justice and Equality* [2016] IECA 362, para. 24.

[197] See, e.g., McIntyre, 'Voluntary Disclosure of Data to Law Enforcement'.

[198] See, e.g., Commission of the European Communities, *Non-paper*, 1, 3–4.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

- disclosure to other jurisdictions was lawful in light of Facebook's legitimate interest in cooperating with law enforcement authorities.[199]

A full assessment of these arguments is outside the scope of this chapter, but there were question marks over them even then. For example, the reliance on section 8(b) to permit disclosure to foreign agencies was misconceived, as this section applied only to offences and court orders enforceable under Irish law.[200] Similarly, Facebook's argument that users consent to data being transferred for criminal investigations was a questionable application of consent under Directive 95/46/EC, and is now unsustainable in light of the heightened standard of consent in Article 7 GDPR.[201]

The lack of transparency in this area makes it difficult to assess, but in principle voluntary disclosures within the EEA might be permissible on the same conditions as domestic disclosures, discussed earlier in Section 12.4.3. The additional question that arises in the cross-border context is whether a voluntary disclosure for law enforcement purposes can be made to a third country in a way that is compatible with Chapter V of the GDPR.

It is difficult to see how these voluntary disclosures to third countries for law enforcement purposes could be legitimated. None of the relevant Article 49 GDPR derogations would appear to be available. User 'consent' in terms of use would not meet the requirements of prior information and explicit consent under Article 49(1)(a) GDPR. The Article 49(1)(e) derogation for transfers 'necessary for the establishment, exercise or defence of legal claims' appears to be limited to cases in which the data controller is closely involved rather than cases where the controller merely holds some evidence;[202] but, even on a wider interpretation, transfers for merely *investigative* purposes would not fall within the derogation.[203] The 'important reasons of public interest criterion' under Article 49(1)(d) will not apply where the public interest at stake is that of a third country; the European Data Protection Board (EDPB) has stressed that it is available only where 'it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation'.[204] As a result, the EDPB has issued guidance: 'In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to [the] existing MLAT or agreement.'[205] In light of this, the practice of voluntary disclosure to non-EEA law enforcement agencies is of questionable legality at best.

12.5.4 *Opportunities and Challenges Created by the e-Evidence Regulation*

In a notable change from a previous policy of opting out of the EIO and other instruments, Ireland has opted into the new e-Evidence Regulation.[206] This is particularly significant owing to

[199] See, e.g., Data Protection Commissioner, *Facebook Ireland Report of Audit*, appendix 5.
[200] Annette Hogan, 'The Interception of Communications in Ireland: Time for a Re-Think' (2014) 7(5) *Data Protection Ireland* 8.
[201] See, e.g., Haase and Peters, 'Ubiquitous Computing and Increasing Engagement', 131–132.
[202] European Data Protection Board (EDPB), *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679* (25 May 2018), 11, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.
[203] Kopp and Pfisterer, 'Between a Rock and a Hard Place', 73; EDPB, *Guidelines 2/2018*, 11.
[204] EDPB, *Guidelines 2/2018*, 10.
[205] Ibid., 5.
[206] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

the presence of many service provider European headquarters in Ireland. Recognising the perception of Ireland as a weak regulator, an internal government memorandum noted: 'There is already a perception in some member states that Ireland is benefitting financially by attracting such international service providers to establish themselves in Ireland but is not willing to properly regulate them, to the detriment of other EU states … Non-participation in the e-evidence proposal will strengthen that view.'[207]

The Regulation entered into force in August 2023, but it will be three years before all aspects of the Regulation fully apply. The extent of the Regulation's implications for Irish practice will become apparent over time, but a few observations can be made at this point. From a fundamental rights perspective, the starting point is that Irish law is in need of significant reform. For example, as we have seen in Sections 12.4.3 and 12.4.5, the lack of notification for users whose data has been accessed[208] and the heavy reliance on voluntary disclosure of data mean that there are key gaps in regulation. In principle, the e-Evidence Regulation offers an opportunity to remedy these problems – for example, it will introduce independent approval for access to traffic and content data, which at the moment can be accessed by voluntary cooperation without any judicial control. Consequently, aspects of the package would represent a significant improvement on the Irish legal framework. Against that, however, the Regulation will do nothing to enhance the legal certainty or protection of fundamental rights if it becomes simply an additional layer that leaves the existing legal instruments and voluntary cooperation practices in place underneath.

Specific challenges to the operation of the Regulation's safeguards may arise in Ireland owing to the high number of service providers headquartered in the state. The Regulation's reliance on a notification process[209] – where the enforcing authority in the service provider's country of establishment has only ten days (ninety-six hours in an emergency) to raise a ground for refusal of a production order – clearly prioritises efficiency.[210] Considering the outsized number of requests likely to be received by the competent Irish authority and the short time limits to raise a ground for refusal, the ability of the enforcing authority notification requirement to provide effective protection remains in question.[211]

From the perspective of providers, the Regulation also significantly increases their burdens. For example, the requirement that in emergency cases data must be transmitted within eight hours has no parallel under existing Irish law, which usually gives providers seven days to comply with a mandatory order to disclose data.[212] The sanctions for failure to provide information – up to 2 per cent of worldwide annual turnover – are several orders of magnitude greater, and are exacerbated by the limited grounds on which a disclosure requirement can be challenged.[213] At the moment providers based in Ireland typically have a 'reasonable excuse' defence for failure to comply with an interception warrant, search warrant or production order; the Regulation, by taking a 'de facto impossibility' approach, will make it more difficult to defend a failure to provide data based on issues of technical difficulty or conflicting legal obligations.[214]

[207] Fiach Kelly, 'Government Told to "Properly Regulate" Internet Giants', *Irish Times*, 9 July 2018, www.irishtimes.com/news/ireland/irish-news/government-told-to-properly-regulate-internet-giants-1.3558281.

[208] Except in relation to Schedule 2 data under the Communications (Retention of Data) Act 2011.

[209] Reg. 2023/1543, Art. 8.

[210] Ibid., Art. 12.

[211] Valerie Albus, 'Fast-Tracking Law Enforcement at the Expense of Fundamental Rights', *Verfassungsblog*, 15 June 2023, https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights/.

[212] Reg. 2023/1543, Art. 10; Francisco and Rosenkranz, 'United States of America v. Microsoft Corporation', 37.

[213] Reg. 2023/1543, Art. 15.

[214] Ibid., Arts. 16(4)(c) and 16(5)(b). The risk of legal conflicts is partially mitigated by the review procedure in the event of conflicting obligations set out in Article 17. The Regulation also makes reference to denying an order on the basis

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

Finally, it is not clear that the Regulation itself will significantly improve the position for Irish law enforcement. It is limited to cross-border cooperation, with production and preservation requests to domestic service providers still being subject to national law. With many of the main internet firms having their Europe, Middle East and Africa (EMEA) headquarters in Ireland, Irish police may not get much practical benefit from the Regulation; national law, with all the problems outlined already, would still be more important. In addition, the Regulation does nothing to address the problem of admissibility, so that police in Ireland may end up with faster access to material for investigative purposes but continue to face issues in using that material for prosecution purposes. Consequently, it will be important to see how far domestic implementing legislation goes beyond the Regulation itself. At the time of writing (February 2024), proposed legislation to implement the Regulation has just been published and is about to enter pre-legislative scrutiny.[215]

12.6 CONCLUSION

The issue of access to digital evidence is of fundamental importance in Ireland, but the dated legal framework, the lack of adequate oversight and the lack of transparency around the activities of the Irish authorities and providers with an Irish presence make it difficult to assess Irish law in this area. Where we do have detailed information on how access to data operates in practice – from the Facebook audit and the Murray report – it has been the result of ad hoc investigations into particular scandals. But the material that is publicly available makes it clear that reform of the law on access to data is long overdue. Between the invalidation of data retention, the need for modernisation of interception and the e-Evidence Regulation, there is pressure from all directions on the existing framework.

Despite these factors, the state has largely failed to act. The Department of Justice has yet to present any coherent plan to modernise Irish law. Instead, the strategy to date has been one of kicking the can down the road. This failure would be notable even if its effect were merely domestic, but it is magnified by the fact that it also impacts hundreds of millions of users elsewhere whose data is stored and managed in Ireland. By encouraging internet firms to establish in Ireland, the state has taken on a responsibility to properly regulate access to the data of their users – and that responsibility is not being met. Without a transparent reform process that respects the European privacy and data protection framework, Irish law will continue to fail both the protection of fundamental rights and the public interest in effective investigation of crime.

of 'immunities or privileges granted under the law of the enforcing State, or [where] the data requested are covered by rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media' and provision for denial in 'exceptional situations' where it is apparent that there are substantial grounds to believe, 'on the basis of specific and objective evidence', that the execution of the order would entail a 'manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter' (Reg. 2023/1543, Arts. 16(4)(f)–(g) and (5)(e)–(f)).

[215] Department of Justice, 'Ministers McEntee and Browne Receive Approval to Draft Legislation to Allow Gardaí Swift Access to Digital Criminal Evidence', 7 February 2024, www.gov.ie/en/press-release/81d45-ministers-mcentee-and-browne-receive-approval-to-draft-legislation-to-allow-gardai-swift-access-to-digital-criminal-evidence/.

Downloaded from https://www.cambridge.org/core. University College Dublin, on 12 Dec 2025 at 10:46:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009049771.014

APPENDIX 3

An tSeirbhís Chúirteanna
Courts Service

Mr Alan Guidon
Clerk to the Committee
Joint Committee on Justice, Home Affairs and Migration
Leinster House
Dublin 2

5th December 2025

Your Ref: JC/7/1/G/1

Dear Alan,

I refer to your letter of 11 December 2025 on behalf of the Joint Oireachtas Committee on Justice, Home Affairs and Migration inviting the Courts Service to give a written submission on the General Scheme of Criminal Justice International Cooperation Office Bill 2025. I welcome the opportunity to assist the Committee.

The Department of Justice, Home Affairs and Migration brought this Scheme to the attention of the Courts Service earlier this year and sought our views on its operational impact. We met the Department on a number of occasions to discuss this Scheme and the related General Scheme of Criminal Justice (Protection, Preservation of and Access to Data on Information Systems) Bill 2024 (the 2024 Bill). There are plans for further engagement with the Department in the new year.

From this engagement, it seems the impact of this General Scheme is limited as the majority of applications to the International Cooperation Office will need no involvement of a Court. There are provisions of the Scheme that I wish to address and I do so in the attached submission.

While this Scheme is not expected to have a significant impact on the Courts in isolation, I have concerns about the impact of the broader legislative programme addressing data issues and also the outcome of the decision of the European Court in the Dwyer case (Case C140-20). The central role that Courts are to play in managing applications relating to data access will need careful planning and resourcing if it is not to impact on other areas of Court activity.

Data related proceedings are and will continue to grow with the commencement of this Scheme, the 2024 Bill, planned new regulations to support the Irish Passenger Information Unit and also the Communication (Retention of Data) (Amendment) Act 2022 which is already operational.

If you require any further information or any clarification, please let me know.

Yours sincerely

Angela Denning
Chief Executive Officer

Aingeal Ní Dhuinnín, Príomh Fheidhmeannach, AN tSEIRBHÍS CHÚIRTEANNA, Áras an Fhionn Uisce,
15/24 Sráid an Fhionn Uisce Thuaidh, Margadh na Feirme, Baile Átha Cliath 7 D07 F95Y.
Angela Denning, Chief Executive Officer, COURTS SERVICE, Phoenix House, 15/24 Phoenix Street North, Smithfield, Dublin 7 D07 F95Y.
Teileafón/Telephone: 01 888 6426 Ríomhphost/Email: officeoftheceo@courts.ie Láithreán Gréasáin/Website: http://www.courts.ie

Submission on

Criminal Justice International Cooperation Office Bill 2025

1. This is a new area of activity for the Courts, and currently there is limited data available on the number of cases that may arise after commencement. Discussions with the Department of Justice, Home Affairs and Migration (DJHAM) suggest that the volume of cases is expected to be low, as service providers are not anticipated to challenge decisions of the Criminal International Cooperation Office on a large scale. This expectation appears to be informed by DJHAM's consultations with service providers and previous experience in similar contexts where data was sought. That said, the Courts Service acknowledges that this projection may prove optimistic, and the situation may need to be reviewed post -commencement.

2. Head 4.7 - Appeal against decision and penalty.
   This head provides a mechanism for parties to appeal a decision of the Director of the Office of Criminal Justice International Cooperation. The appropriate jurisdiction for appeals is based on the monetary value of the financial penalty imposed on the appellant. The High Court is the appropriate Court to hear appeals unless the penalty does not exceed €75,000 in which case the matter will be heard by the Circuit Court. While it is expected that the number of appeals will be low, some cases may be complex and could require significant court time, particularly where penalties involve substantial sums.

3. Head 4.8 – Circuit Court confirmation of decision.
   This provision is similar to those in recent legislation (e.g., Gambling Regulation Act 2024, Health (Assisted Human Reproduction) Act 2024), where a Court is required to confirm a decision of a new agency. The Courts Service is unclear on the necessity of this requirement. Where a party is dissatisfied with a decision of the Director, an appeal process is already available to challenge its validity. Requiring a Court to confirm an uncontested decision may not be the most efficient use of resources.

4. New Offences
   The Bill creates certain new offences (for example under Head 4.2 and Head 4.6) Summary offences are to be prosecuted by the Director. There is limited information on the number of potential prosecutions that may arise under these offences (either summary or indictable) therefore at this time it is difficult to quantify the potential impact on the criminal courts.