

CHECK AGAINST DELIVERY

**Presentation by the Independent Examiner of Security Legislation,
George Birmingham**

Office of the DPP

Tuesday 8 September 2026

Good afternoon.

The origins of the Office of Independent Examiner of Security Legislation (IESL) can be traced to the Commission on the Future of Policing (the Commission) which was established in 2017 under the chairmanship of Kathleen O'Toole, one-time head of the Garda Inspectorate, which reported in September 2018.

One of the many issues that the Commission addressed was whether gardaí should continue to have a dual role as a police force and a security service; the Garda Síochána is unusual in having a dual role as it does. Across Europe, and indeed across the common-law world, dedicated security and intelligence services are the norm.

After much debate (it appears some of which was heated), the Commission recommended in favour of the retention of the status quo. However, they did so subject to certain caveats or qualifications. They recommended that the security and intelligence capability of An Garda Síochána should be strengthened by means of a ring-fenced budget provision, and also

by giving the agency the ability to recruit specialist operatives with relevant analytical, technological and legal skills, and to do so directly and quickly. The Commission explained that they felt there was a need for special arrangements to address the issue of oversight of national security. They believed there were two reasons why special arrangements were required in this area.

Firstly, they acknowledged that national security by its very nature involves highly sensitive information – intelligence emanating from sources that need to be protected, and from liaison services whose product must be handled with particular care. Secondly, they commented that the oversight bodies, instancing in that regard the Policing Authority and GSOC, had expressed concerns about the fact that their request for information was sometimes being met with resistance on grounds of national security. The oversight bodies were of the opinion that national security was being invoked more widely than was necessary. The Commission also expressed the view that there was a need for a comprehensive and robust review of the legislative framework within which police and other agencies operate in the area of national security.

The Commission then recommended the establishment of an “Independent Examiner of Terrorist and Serious Crime Legislation”, a recommendation which they said they were making very specifically based on the model that existed in the UK. They commented that the Examiner would maintain a continuous review of how security legislation was being implemented by police and other agencies, and evaluate the case for changes needed to match evolving threats while respecting fundamental rights. This, they made clear, would require the Examiner to have the power to

review the conduct of particular security operations when concerns arise, calling for independent scrutiny.

Significantly, the Commission also observed that the Independent Examiner could act as an adjudicator to consider requests for information from policing oversight bodies that had been rejected, in whole or in part by AGS, on grounds of national security. So far as the job specifications were concerned, they were of the view that the Examiner should report to the Taoiseach, and that the appointment should be a part-time one. They commented that selecting the right individual would be crucial. A strong legal background along with great credibility within the legal profession would be necessary, but excellent communication skills would also be very important [*time for an aside here*].

The Commission looked to the United Kingdom for a model to draw upon. There the role of Independent Reviewer of Terrorism Legislation is well established. The first reviewer of the Terrorism Act 2000, which had consolidated anti-terrorism powers into a single, comprehensive code and had made permanent those powers, was Lord Alex Carlisle, QC, a former Liberal Democrat MP. He fulfilled the role for nine years. During his time in office, he visited Ireland on a number of occasions, taking a particular interest in how the Special Criminal Court operated. I met with him on occasion in Green Street courthouse where trials were taking place where I was prosecuting, meeting him at the request of the then DPP, the late Eamon Barnes. The current Independent Reviewer is Jonathan Hall, KC. He was appointed in May 2019 when his predecessor, Sir Max Hill, was appointed to be DPP after 18 months as Reviewer. Jonathan Hall, as many of you will be aware,

has developed a significant public profile, though probably the most high-profile and best-known holders of the office was David Anderson, Baron Anderson of Ipswich, no stranger to this office as he was called to give evidence on behalf of the State in the course of proceedings brought by Graham Dwyer, challenging the regime in place to access retained data records.

While Alex Carlisle was the first person to have a formal role as Independent Reviewer, the idea of the involvement of independent figures in the formulation of terrorism legislation goes back much further, and has its origin in the Troubles in Northern Ireland. Back in 1972 a commission chaired by Lord Diplock, a serving Law Lord, was asked to report on what arrangements could be made "in order to deal more effectively with terrorist organisations by bringing to book, otherwise than by internment by the executive, individuals involved in terrorist activities". The result of that exercise was the establishment of the nonjury Diplock courts. There was a number of other interventions, including a commission chaired by Lord Gardner, the former Labour Lord Chancellor, which made a large number of recommendations, including controversially that Special Category Status for Prisoners convicted of scheduled offences should be ended. In 1996 Lord Lloyd, another serving Law Lord, made recommendations which would form the basis of the Terrorism Act 2000, a permanent piece of legislation.

The recommendations of the Commission were given effect to by the Policing, Security and Community Safety Act of 2024, and in particular by part seven thereof. That legislation came into force on 2 April 2025 with the formal establishment of the office, though I had been designated in October 2024 as the first Independent

Examiner of Security Legislation. The legislation sets out the objectives, powers and functions of the office. Statute stipulates that the objectives of the Independent Examiner shall be to:

- (i) provide public confidence in security legislation;
- (ii) support the Government in protecting the security of the State;
- (iii) ensure that information relating to his or her function is made available to the public to the greatest extent possible, without prejudicing the security of the State, defence or international relations; and
- (iv) ensure that his or her functions are performed in a timely, efficient or effective manner.

Section 234 (2) provides that the Independent Examiner shall have the following functions:

- a) to keep under review the operation and effectiveness of security legislation, including by examining whether the security legislation is effective and proportionate in its objectives insofar as they relate to the protection of the security of the State and contain sufficient safeguards for the protection of human rights.
- b) the legislation designates seven statutes as security legislation to be reported on regularly. Three pieces of legislation, namely the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993; the Criminal Justice (Surveillance) Act 2009, and the Communications (Retention of Data) Act 2011 are to be

reported on annually while the remaining four: the Offences Against the State Act 1939 - 1998, the Criminal Law Act 1976, the Criminal Justice (Terrorist Offences) Act 2005 and the Criminal Justice (Money Laundering and Terrorist Offences) Act 2010 are to be reported on at least once every three years.

The distinction between the legislation required to be reported on annually and the balance of the list is that the measures requiring at least annual review all involve the exercise of powers of an intrusive nature on an ongoing basis where the powers were conferred by statute. It is also the case that the three pieces of legislation, subject to annual review, were all subject in the past to judicial oversight by a designated judge. In practice, what happened in the past typically involved an annual visit by the designated High Court judge in order to examine a representative sample of files selected by him or her. That practice has now changed since I took up my role. I now visit each of the agencies exercising statutory powers once a quarter, and it is my practice to ask to see all relevant files and not just a representative sample.

Another important feature of the Office of Independent Examiner is that I have a role in carrying out a review of a refusal by the Garda Commissioner to provide information sought or a document requested to the Policing Authority or the Garda Ombudsman or an objection by the Commissioner to a search of Garda premises, if the refusal by the Commissioner on the grounds of national security is appealed by the relevant oversight body. If there is a dispute the matter is referred to me and I make a recommendation to the Minister for Justice.

Apart from the three areas that were subject to annual oversight by designated judges which I have inherited, there is one other area where the judiciary, or more accurately retired members of the judiciary, had a role. Garda activity in relation to CHIS had for a number of years been the subject of oversight, though on a non-statutory basis. The role is filled currently by retired President of the Circuit Court, Ray Groarke and before that it was dealt with by Garrett Sheehan. It became clear to me how significant for garda operations was the interaction with CHIS, so I asked for and received a detailed briefing in this area.

Postal and Telecommunication interception

The lawful interception of postal and telecommunications in Ireland is dealt with by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

While the legislation dates from 1993 that is not to say that interception commenced only in that year. In a report in Britain in 1957 by a group of privy councillors, the Birkett Report, they commented that the origin of the power to intercept was obscure, but they were able to point to a Royal proclamation from 1663 that outlawed interference with post except under a warrant of the Secretary of State.

Two court decisions, one of the High Court and one of the ECtHR, provide the backdrop to the legislation. The High Court case, that of Kennedy and Arnold v Ireland, arose from the tapping of the phones of two leading journalists prominent in the political sphere. At the Strasbourg level, Malone v UK was also of major significance. In that case the ECtHR found that the issuing of

warrants on a non-statutory basis, which provided for interception of communications, was in breach of the applicant's right to respect for his private life and also concluded that the interference was not “in accordance with law”. It was abundantly clear that the criticisms by the ECtHR in Malone of the situation in the UK would also apply with equal force to what was happening in this jurisdiction. The Act makes provision for the Minister for Justice, Home Affairs and Migration to authorise interceptions, but he can do so only for the purpose of criminal investigation or where interception is in the interests of the security of the State. It might be noted that there is provision in the statute for the Minister to consult with the Independent Examiner before deciding whether or not to issue an authorisation. That has not happened during my time in office.

The conditions which must apply before an authorisation can be issued are set out in the statute. In the case of interceptions in support of a criminal investigation, it is required that investigations are being carried out by An Garda Síochána, the Police Ombudsman or another public authority charged with the investigation of offences concerning a serious offence or a suspected serious offence. It must be the situation that investigations have failed or are likely to fail to produce results and there is a reasonable prospect that interception would be of material assistance in providing information or evidence. In cases involving State security it is required that there are reasonable grounds for believing that particular activities are being carried out, or proposed to be carried out, which are endangering or are likely to endanger the security of the State.

The Act also deals with the procedures for applying for an authorisation. In cases of criminal investigations, it requires that an application must be made by the Garda Commissioner or the Police Ombudsman. In cases involving the security of the State the application may be made by either the Garda Commissioner or the Chief of Staff of the Defence Forces. Applications are required to be in writing and are submitted to a nominated officer of the Minister, a very senior officer in the Department of Justice. If an application is being made by the Chief of Staff of the Defence Forces it must be accompanied by a written recommendation from the Minister for Defence, supporting the application. The Act provides for a complaints procedure and creates the office of Complaints Referee, an office now held by Judge Dara Hayes.

The Act is seriously out of date, something which has been commented on publicly by a number of the holders of the office of designated judge over the years. Perhaps the most significant deficiency is the fact that the legislation predates modern digital communications, thus providing only for the interception of voice, SMS (short message service) and MMS (multimedia messaging services). The Act makes no provision for the interception of databased or over-the-top (OTT) services such as WhatsApp, Telegram or Snapchat, to mention just a few. There is no legislative basis to access the content of databased material, such as webpages or internet browsing history through interception. In the case of postal interception, the legislation only covers An Post and not couriers or other delivery services. Unlike more modern statutes which regulate the exercise of intrusive powers, there is no provision for judicial authorisation [*Possible reference to AG v Edison Telephone Company*].

I suspect that the area of lawful interception is the area involving intrusive powers which the people in this room, in this office, have least direct contact with. This is because interception has always been undertaken for intelligence purposes. There has never been, so far as I know, any attempt to put the product of the interception into evidence in the course of a trial. While that is so, one of the conditions required for authorisation of an interception is that investigations not involving interception have failed or are likely to fail to produce (a) information to show whether the offence has been committed or as to the facts relating to it; (b) evidence for the purpose of criminal proceedings relating to the offence. Again, this statute talks about reasonable prospects of an interception providing information or evidence.

The situation is more clear cut in Britain. There the Investigative Powers Act 2016 contains a specific statutory bar on the use or disclosure of the product of a targeted interception warrant during the course of legal proceedings. That has been the situation since interception was first placed on a statutory basis in 1985, but the issues have proved controversial. In 2007 the Government established a Privy Council review to advise whether a regime to allow for the use of intercepted material in court could be devised that would facilitate bringing cases to trial while meeting the overriding imperative to safeguard national security. The review concluded, with some obvious hesitation, that the product of interception should in principle be admitted as evidence and that it would be possible to draw up a statutory scheme which would permit this. However, when the group of privy councillors was reconstituted as an advisory group to move matters forward, the

view was taken that legal requirements for making such provision would result in potential miscarriages of justice, more expensive and complex trials, and more guilty defendants walking free so the status quo of non-admissibility was maintained.

Surveillance

In contrast with the reality that the product of lawful interception is not put in evidence in the course of trials, the Criminal Justice (Surveillance) Act 2009 is of direct and daily relevance to the work of this office. The legislation was introduced against a background of significant public concern at what was seen as a significant, if not indeed dramatic, increase in organised crime. Of note for our purposes is that when introducing the legislation in the Dail, the then Minister for Justice, Dermot Ahern, stated that “the primary purpose of the legislation is to facilitate the use in evidence of material gained by means of secret surveillance in criminal proceedings”.

While the Minister may have seen that as the primary purpose, there is no doubt that surveillance is also undertaken pursuant to statute for intelligence gathering purposes. O'Malley, J in the course of her judgment in DPP v Hanaway made the point that while that appeal was concerned with the exercise of statutory powers for the purpose of criminal investigation, the statute also clearly contemplated the gathering of information for intelligence purposes. The title of the act, and indeed the long title is a broad one, but despite that, the remit of the 2009 Act is much more confined than might at first appear with much of what would generally be regarded as surveillance activity falling outside its scope. This arises from the definition of surveillance. It is defined

as “monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or by monitoring or making a recording of places or things **by or with the assistance of a surveillance device**”. This reference to “by or with this system of a surveillance device” in the definition is critical. It means that covert, or for that matter, overt surveillance which involves following or observations without the deployment of a surveillance device falls outside statutory regulations. Our restricted statutory definition with its focus on the deployment of surveillance devices is to be contrasted with the approach taken in the UK. There the definition set out in the Regulation of Investigatory Powers Act 2000 is stated as including (a) monitoring, observing, or listening to persons, their movements, their conversations, all their other activities or communications; (b) recording anything monitored, observed or listened to in the course of surveillance; and (c) surveillance by or with the assistance of a surveillance device, but the definition does not purport to be exhaustive and the monitoring, observing, or listening doesn't have to be recorded, and doesn't have to involve the use of technology in order to come within the statutory definition.

The Act applies to surveillance carried out by members of An Garda Síochána (AGS), designated officers of the Police Ombudsman, members of the Defence Forces, officers of the Revenue Commissioners and authorised officers of the Competition and Consumer Protection Commission. The Act provides that members of the relevant bodies carry out surveillance only in accordance with a valid authorisation or an approval. The procedure for applications is set out in the statute. It provides that specified senior

figures within the various bodies may apply to a judge of the District Court for an authorisation. In the case of An Garda Síochána, a senior officer is defined as being someone not below superintendent level. He or she may apply if they have reasonable grounds for believing that as part of an operation or investigation being conducted by An Garda Síochána concerning an arrestable offence the surveillance being sought to be authorised is necessary for:

- the purpose of obtaining information as to whether an offence has been committed,
- or as to circumstances relating to the crime or is necessary for the purpose of obtaining evidence,
- or that the surveillance is necessary for the purpose of preventing the commission of an arrestable offence,
- or that the surveillance being sought is necessary for the purpose of safeguarding the security of the State.

There are similar provisions in relation to the Police Ombudsman where the superior officer is defined as a superior designated officer. In this case, applications for authorisation are in the context of investigations being conducted by the Police Ombudsman into arrestable offences. Again, there are similar provisions in relation to the Revenue Commissioners and the Competition and Consumer Protection Commission. In these cases, the senior officer is defined as being a person not below the rank of Principal Officer. In the case of Revenue, applications are in the context of investigations of Revenue offences, while in the case of the CCPC the application is in the context of cartel offences.

For completeness, while not directly relevant to the work of the DPP, I should mention that there is provision for a superior officer of the Defence Forces, defined as being not below Colonel rank making application to the District Court for an authorisation where he or she has reasonable grounds for believing that the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State.

When authorisations are granted, they are for the period fixed by the District Judge but that period cannot exceed three months, but there is provision for renewal or variation.

There is also provision in the Act at Section 7 for internal approvals in cases of urgency. Surveillance under this urgency regime is limited to 72 hours. If the superior officer who issued the initial urgent authorisation believes that an authorisation beyond 72 hours is warranted, then he or she makes an application to a judge for continuation.

Of note is that the regime that applies in the case of tracking devices is quite different. Movements of persons, vehicles or things may be monitored without prior judicial authorisation. Members of the bodies vested with statutory powers may apply to a superior officer for the grant of an approval to deploy a tracking device. Though the view has been taken that the deployment of a surveillance device is less intrusive, and does not require prior judicial authorisation, in the course of my first annual report, I expressed some discomfort with this approach. I queried the assumption that information from a tracking device about an individual will be limited and felt that the view that it is not really intrusive is questionable. I suggested that consideration should be given to the question of whether it remains appropriate to provide

for the deployment of tracking devices without prior judicial authorisation. I qualified this by saying that if the view was taken that requiring prior independent judicial authorisation on a blanket basis placed too great a burden on those exercising the powers and would prove impractical, that consideration might be given to a two-tier approach, which would permit the use of tracking devices for a short period on the basis of internal approval, with the requirement to then seek a judicial ratification.

The Government's response to my report indicated an openness to the suggestion, stating that the recommendation would be considered in the context of an ongoing review of the framework for intrusive powers, and that in developing any proposals consideration would be given to the period of time after which judicial authorisation would be required.

You will probably be interested in knowing how frequently powers are exercised. During the period covered by my first report from establishment day on 2 April to 31 December 2025, An Garda Síochána made nine applications to the District Court for authorisations, all of which were granted, and eight applications for variations or renewals. The figures for the previous year were comparable to the period of my review, and during the review period and indeed the previous year the gardaí did not avail of the Section 7 urgency procedure. Tracking devices were deployed on 47 occasions during the period under review. During the review period, the Revenue Commissioners made three applications to the District Court, up from only one in the previous calendar year. Revenue deployed tracking devices on 21 occasions during the period under review, very much in line with the previous year, when the figure was 22. For completeness, and as mentioned earlier,

probably not of direct relevance to this Office, I should indicate that the Defence Forces made six applications during the period under review. Fiosrú did not exercise their powers during the period under review. In the case of the CCPC, they had only recently acquired statutory powers in this area and were engaged in making the necessary preparations in order to exercise those powers.

Communications (Retention of Data) Act

The Communications (Retention of Data) (Amendment) Act 2022 is, I suspect, of greatest significance for this office on a day-to-day basis. The background to where we find ourselves today is a complex one. In 2011 the Oireachtas enacted the Communications (Retention of Data) Act 2011 to give effect to the Data Retention Directive. In the light of subsequent developments, it is worth reminding ourselves that Ireland was in no great hurry to ratify the directive. Indeed, Ireland was brought to the CJEU by way of enforcement proceedings by reason of a failure to transpose. Ireland also launched a challenge to the Directive, contending that criminal investigation was not an EU competence.

Be that as it may, eventually Ireland did move to transpose the directive doing so by enacting the Communications (Retention of Data) Act 2011. At the heart of that legislation was a requirement for all service providers to retain fixed network telephony and mobile telephony data for a period of two years. The provisions of the 2011 Act were then challenged before the Irish courts in the case of Digital Rights Ireland v the Minister for Communication, that resulted in a reference to the CJ EU, raising questions as to the validity of the Data Retention Directive. The court concluded that the directive was invalid, observing that it caused a “wide-ranging” and “serious interference” with the rights to privacy and data

protection. In a series of cases that followed, the court held that national legislation that provided for general and indiscriminate retention of all traffic and location data of all users of electronic communication services relating to all means of electronic communications, and imposing a duty on service providers to keep all data, without exception, went beyond what was necessary and proportionate.

In this jurisdiction, the question of whether subsequent to the annulment of the 2006 directive, the 2011 Act was compatible with EU law came into sharp focus in the course of a number of high-profile criminal trials, most particularly the trial of Graham Dwyer and the associated litigation. The legislative response to these developments was the enactment of the Communications (Retention of Data) (Amendment) Act 2022 Ac, the purpose of which was to amend the 2011 Act in order to achieve conformity with the jurisprudence of the CJEU in the area of general and indiscriminate retention of communication data for reasons of national security and for criminal law enforcement purposes.

The Act categorises data as user data, Schedule 2 data, more commonly referred to as traffic and location data and internet source data. User data includes user ID, the name and address of a subscriber, mobile or fixed telephone number, the International Mobile subscriber identity (IMSI), the International Mobile equipment identity (IMEI). Schedule 2 data or traffic and location data is the data necessary to trace and identify the source of the communication, the destination of the communication, the time and date of the start and end of the communication, the type of communication, communication equipment, the calling and called telephone numbers, the IMSI, and IMEI of the calling and called

parties. In the case of prepaid anonymous services, the date and time of initial activation and the cell ID from which the service was activated, along with the data necessary to identify the location of the mobile equipment. The cell ID at the start of communication and cell ID during the period of communication; the cell ID being the identity of the cell from which a mobile telephone call originated or in which it is terminated.

Internet source data is defined as “the following data necessary to trace and identify the source of a communication by Internet access, Internet, email or Internet telephony can see the Internet protocol (IP) address, whether dynamic or static, allocated by the service provider to the source of a communication”. The name and address of the subscriber or registered user to whom an Internet protocol (IP) address was allocated at the time of the communication.

The legislation provides for different regimes for retention and access in each case. In the case of access there is essentially a tiered approach with the provisions applicable to internet source data and Schedule 2 data being more demanding and those in relation to user data being less so. The general position is that user data can be accessed on foot of a requirement to service providers by persons of specified seniority within the bodies possessing statutory powers in the area, while access to internet source data and Schedule 2 data normally requires prior judicial authorisation, though provision is made for expedited and simplified procedures in cases of urgency.

In addition to the distinctions drawn on the nature and categorisation of the data there is a second differentiation based on the purpose for which access is sought, with a distinction drawn

depending on whether what is an issue is State security, or whether what is an issue relates to a criminal investigation or other permitted purposes. As far as data retention is concerned, the obligation to retain user data is dealt with at Section 3. Service providers are required to retain data for a period of one year or such period as may be prescribed by regulation. The situation in relation to the retention of Schedule 2 data is less straightforward. It is dependent on whether a “relevant judge” of the High Court has made an order under section 3A, (as inserted by section 4 of the 2022 Act) in the context of a threat to the security of the State on foot of an application brought to the court by the Minister. Statute provides that the Minister, when satisfied that there exists a serious and genuine present or foreseeable threat to the security of the State, may make an application to a relevant judge for an order. The application is made ex-parte and by statute and is heard otherwise than in public. Orders under this section have been made in late June 2023, 2024, 2025 and 2026.

As far as user data disclosure is concerned a member of An Garda Síochána not below the rank of superintendent may require a service provider to disclose to the member user data, where the member believes that the data relates to a person whom the member suspects on reasonable grounds of having committed an offence, or presenting an actual or potential threat to the security of the State or where the member has reasonable grounds for believing that the data is otherwise required for the purpose of:

- (i) preventing, detecting, investigating or prosecuting offences;
- (ii) (ii) safeguarding the security of the state;

- (iii) (iii) protecting the life or personal safety of a person in circumstances where the member believes that there is a serious risk to the life or personal safety of the person; or
- (iv) (iv) determining the whereabouts of a missing person. There are comparable provisions in relation to the Revenue Commissioners and the Competition and Consumer Protection Commission.

For completeness, a member of the permanent Defence Forces not below the rank of Lt Colonel may require the disclosure of user data where the officer believes that the data related to a person whom the member suspects, on reasonable grounds, of presenting an actual or potential threat to the security of the State or where the member has reasonable grounds for believing that the data is otherwise required for the purpose of safeguarding the security of the State.

Somewhat surprisingly, the Act makes no specific reference to Fiosrú or to the Police Ombudsman. In my report I described that as surprising and indeed unsatisfactory. I referred to the fact that Fiosrú and its predecessor have a long history of activity under the 2011 Act. Accordingly, one would expect that, given the intrusive nature of the powers provided for, there would be absolute clarity as to what bodies are exercising powers. I pointed out the distinction with other areas, such as lawful interception and surveillance, which include a specific reference to a role for the Police Ombudsman.

A significant feature of the legislation is that it provides for the creation of two new types of legal orders; preservation and production orders. For these two orders the norm is by way of an

application to an authorising judge, though provision is made for situations of urgency through temporary preservation and temporary production orders. The preservation order was described by the Minister for Justice of the day when commencing the Act as a “quick freeze”. The purpose for which the preservation or production order is sought will determine what data can be the subject of the order. Where access to the data is sought on grounds that the person making the application, believes that the data relate to a person whom the member suspects on reasonable grounds of presenting an actual or potential threat to the security of the State or as otherwise required to be preserved for the purpose of safeguarding the security of the State, such data will include data stored, retained or otherwise within the possession or control of the service provider under a contractual obligation, or pursuant to a court order, **including** an order under Section 3a or a preservation order under subsection 4. On the other hand, if the data is sought for purposes other than State security, then the data that can be accessed includes data stored under a contractual obligation or pursuant to a court order other than an order under Section 3a. The critical point here is that data which the service providers have been obliged to retain by reason of the Section 3a order will not be the subject of a preservation order or production order when that order is sought for reasons other than State security.

The various judgments of the CJEU, to which I made a passing reference at the start of this section of my remarks, gave rise to a degree of despondency on the part of investigators who were initially of the view there was no longer any real scope for seeking and obtaining traffic and location data. It is very much to their credit that those involved in the area at Garda headquarters took the view

that the decisions had not brought to a shuddering end the prospect of seeking information but placed a premium on moving with maximum expedition. They brought their message in that regard to investigating gardaí across the country and are greatly to be commended for that.

So far as the frequency of resort to this legislation is concerned during the review period, that is to say between 2 April and 31 December 2025, all of the agencies vested with statutory powers, including Fiosrú, with the exception of Revenue Commissioners and the Competition and Consumer Protection Commission, exercised those powers. In the case of An Garda Síochána during the period under review there were 1,292 requests for user data, 403 requests for internet source data and 32 requests for cell site location data. There were nine preservation orders sought and 116 production orders, and these figures show a modest increase level of activity in 2024. The Defence Forces made 83 requests for user data during the period under review. Fiosrú made 27 user data requests and two applications for production orders.

The Future

*Criminal Justice (Money Laundering and Terrorist Financing) Act /
The Terrorist Offence Act / Espionage / Official Secrets Act*