Oifig an Scrúdaitheora
Neamhspleách um
Reachtaíocht Slándála

Office of the Independent
Examiner of Security Legislation

Annual Report of the Independent Examiner of Security Legislation

2025

Contents

Foreword by the Independent Examiner of Security Legislation

I am honoured to have been invited to take on the role as first Independent Examiner of Security Legislation, a newly created statutory office. I am pleased to submit this, my first annual report under section 244 of the Policing, Security and Community Safety Act 2024, incorporating reports on three pieces of security legislation, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, the Criminal Justice (Surveillance) Act 2009 and the Communication (Retention of Data) Act 2011, as amended.

Few people will question the need for security legislation designed to protect the security of the State and to combat serious crime; the legislation required to be reviewed addresses both issues. However, there can be legitimate concern whether overreach is possible and whether legislation sufficiently addresses matters in relation to the safeguarding of human rights and civil liberties. A failure to have sufficient regard for human rights and civil liberties concerns may mean that the legislation is less effective than intended and ultimately may leave Ireland a less safe, less secure and less free, tolerant and democratic State.

The threat the country faces has evolved and broadened in recent years. While for much of the State's history, security concerns, and certainly security legislation focused primarily, indeed almost exclusively, on the threat to the State posed by the IRA in its various manifestations. Now the threats are multipronged. Dissident republicans remain a real concern even more than 27 years after the signing of the Good Friday Agreement, but the threats we face are far broader now. Today, Islamist terrorism is a significant cause of concern, either because of the possibility of attacks within this jurisdiction – and there have been a number of such attacks within the past number of years – and also the possibility of an attack on a neighbouring jurisdiction being planned or launched from this State. There is also the question of extreme right-wing terrorism as well as single issue terrorism and extreme left-wing terrorism. There is also unease about the activities of hostile state actors. The possibility of actions undertaken by so called "lone wolves", whether motivated by terrorist ideology or not, also requires consideration.

Photograph © Nick Bradshaw

All told, the picture that presents is a complex and concerning one. It is appropriate that legislation in this area should be subject to independent examination and review in addition to the need for ongoing, continuous review by the executive arm of Government in order that the public may be confident that the objectives of legislation are being achieved and that is happening, without unwarranted intrusion on human rights and civil liberties.

It is also appropriate that the agencies vested with statutory intrusive powers should be subject to effective external oversight. Since my designation, I have been engaging very regularly with all of the agencies that have been entrusted with statutory powers in this area. I want to express my gratitude to each and every one of them for the cooperation they have afforded me.

In the course of this report, I will be recommending changes designed to strengthen legislation in certain respects and to extend the capacity of agencies working in this area, and I will also be recommending a strengthening of the procedures in relation to the way in which authorisations are sought prior to the exercise of powers. It seems to me that this approach, which I believe is a balanced one, is likely to promote public confidence in security legislation.

I would like to take this opportunity to thank all those who have shared their knowledge, experience and expertise in providing me with a comprehensive picture of the security landscape. Some are individuals or organisations I reached out to, and others took the initiative and contacted me with offers of assistance, in some cases, doing so within days of my designation as the first Independent Examiner.

George Birmingham
Independent Examiner of Security Legislation
April 2026

PART 1

Establishment and Performance of the Office of the Independent Examiner of Security Legislation

1

Overview of the Office of the Independent Examiner of Security Legislation

Functions and Mandate

1.1 The office of the Independent Examiner of Security Legislation ("OIE") is a new statutory body established on 2 April 2025, in accordance with the provisions of part 7 of the Policing, Security and Community Safety Act 2024.

1.2 The Independent Examiner of Security Legislation is an entirely new role and its establishment represents a significant development in Ireland's national security infrastructure, providing as it does for the independent review of security legislation and security services.

1.3 On 15 October 2024, the Government designated me as the first Independent Examiner of Security Legislation.

1.4 On 2 April 2025, the office was formally established when the Policing, Security and Community Safety Act 2024 came into force.

1.5 The legislation, and in particular, part 7 thereof, sets out the objectives, functions and powers of the Independent Examiner. Section 234(1) provides that the objectives of the Independent Examiner shall be:

> "(a) to promote public confidence in security legislation,
> (b) to support the Government in protecting the security of the State,
> (c) to ensure that information relating to his or her functions is made available to the public to the greatest extent possible without prejudicing the security of the State, defence or international relations, and
> (d) to ensure that his or her functions are performed in a timely, efficient and effective manner."

Subsection (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—
> (i) whether security legislation—
> (I) is effective and proportionate in its objectives in so far as they relate to the protection of the security of the State, and
> (II) contains sufficient safeguards for the protection of human rights, and
> (ii) the ongoing necessity of the legislation for the protection of the security of the State;
> (b) to carry out reviews (within the meaning of section 243) and issue recommendations under that section;
> (c) to examine the efficiency and effectiveness of the delivery of security services;
> (d) to prepare annual reports, special reports, and reports under section 246;
> (e) to perform any other functions conferred on the Independent Examiner by or under this Act or any other enactment."

1.6 The legislation provides that subject to the Act, the Independent Examiner should be independent in the performance of his or her functions and also shall have all such powers as are necessary or expedient for the performance of his or her functions.

Reports, Reviews, Referrals and Notifications

Reporting Obligations

1.7 Sections 244, 245 and 246 of the 2024 Act set out the Independent Examiner's reporting obligations.

1.8 Section 244 lists the elements that must be included in the annual report to the Taoiseach, which include annual reviews of the operation and effectiveness of three of the seven Acts of the Oireachtas that are defined as security legislation:

- the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 ("1993 Act")
- the Criminal Justice (Surveillance) Act 2009 ("2009 Act")
- the Communications (Retention of Data) Act 2011 ("2011 Act").

1.9 The operation and effectiveness of the other four enactments designated as security legislation must be reviewed and reported on at least once every three years. These are:

- the Offences against the State Acts 1939 to 1998
- the Criminal Law Act 1976
- the Criminal Justice (Terrorist Offences) Act 2005
- the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

1.10 There is also provision for the Taoiseach to designate other legislation as security legislation.

1.11 Section 245(1) provides that the Independent Examiner may prepare and submit reports to the Taoiseach, in addition to an annual report, on matters relating to his or her activities or the performance of his or her functions, together with any recommendations that the Examiner considers appropriate that, in his or her opinion require, due to the gravity of the matters or other exceptional circumstances, a special report. Section 245(2) provides that the Taoiseach may request the Independent Examiner to prepare and submit a special report:

> "(a) on the actions taken by, or the conduct of, a public body in respect of any incident relating to the protection of the security of the State, or
> (b) in respect of any other matter relating to the functions of the Independent Examiner."

1.12 The legislation also provides at section 246 that the Independent Examiner should "prepare and submit to the Taoiseach, at such times as the Taoiseach may request, a report in relation to the effectiveness of the office, including in respect of the functions of the Independent Examiner" under the 2024 Act itself and also under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, the Criminal Justice (Surveillance) Act 2009 and the Communications (Retention of Data) 2011.

1.13 This first annual report covers the period from establishment day, 2 April 2025 to 31 December 2025. The report contains reference to the period between designation and establishment and also refers to review visits to agencies in 2025 and in the early part of 2026. Once the Taoiseach has laid the annual report before both Houses of the Oireachtas, it will be published bilingually on the OIE website. Under section 244(3) of the 2024 Act, I requested an additional period of four weeks to submit my report. While the text of the report was completed in advance of the statutory deadline, I sought this additional time to allow for the translation of the report in accordance with the requirements of section 10 of the Official Languages Act 2003, and to allow for both versions of the report to be designed to a professional standard. The Taoiseach granted a four-week extension to 28 April 2026.

1.14 In all reports, sensitive information will be appropriately safeguarded by redaction of material for publication, or preparation of an amended report.

1.15 In the reporting period, no special reports were submitted pursuant to section 245, nor were any requests for the preparation of a report made by the Taoiseach in accordance with the provisions set out in section 246.

Processing of Referrals and Notifications under Section 243

1.16 Section 243(1) deals with the role of the Independent Examiner in carrying out a review of the following matters:

> "(a) a refusal by the Garda Commissioner under *subsection (5)* of *section 147*, to comply with a request under *subsection 4* of that section, to provide information or a document to the Authority, (*An tÚdarás Póilíneachta agus Sábháilteachta Pobail*) referred to the Independent Examiner by the Authority under the said *subsection (5)*;
>
> (b) an objection by the Garda Commissioner under *section 210(14)* to a search of Garda Síochána premises, notified to the Independent Examiner by the Garda Commissioner under that subsection;
>
> (c) a refusal by a person under *subsection (5)* of *section 211*, to provide any information, document or thing, pursuant to a requirement under *subsection (1)(a)* of that section or to answer any question under *subsection (4)(a)* of that section referred to the Independent Examiner by the Police Ombudsman under *subsection (7)* of that section;
>
> (d) a refusal by the Garda Commissioner under *subsection (3)* of *section 217* to comply with a request under *subsection (1)* of that section to provide any information or document, referred to the Independent Examiner by the Police Ombudsman under *subsection (4)* of that section."

1.17 From 2 April to 31 December 2025, I received no requests to carry out a review under section 243. However, consideration has been given to the procedures to be followed when the situation arises.

Notification of Incidents of Concern

1.18 If the Commissioner of An Garda Síochána becomes aware of an incident of concern relating to a member of garda personnel, the incident is notified to the Police Ombudsman. If the incident relates to matters that would be prejudicial to the security of the State or would endanger the life or safety of a person who has given information in confidence to a public body in relation to the enforcement or administration of the law (section 204(6)), the Garda Commissioner will limit the information provided to the Police Ombudsman and will notify both the Police Ombudsman and the Independent Examiner (section 204(7)).

1.19 In the period from 2 April to 31 December 2025, I received no such notifications.

Background to the Establishment of the Office of the Independent Examiner

1.20 The origins of the office of Independent Examiner are to be found in the report of the Commission on the Future of Policing in Ireland, published in September 2018. In chapter 11 of that report, titled *Oversight of National Security*, the members of the Commission set out how they saw the need for a comprehensive and robust review of the legislative framework within which police and other agencies operate in the area of national security, what powers they should have, how they exercise those powers so as to respect fundamental rights and what safeguards are in place against abuse or misuse. The Commission commented that as the nature and range of threats to national security are changing fast, as are the technologies in play, it is important that these issues should be under constant review.

1.21 At paragraph three, they recommended the establishment of an Independent Examiner of Terrorist and Serious Crime Legislation, based on the model existing in the United Kingdom. The Independent Examiner would maintain a continuous review of how security legislation is being implemented by police and other agencies and evaluate the case for changes needed to match the evolving threats, while respecting fundamental rights. This would require the Independent Examiner to have powers to review the conduct of particular security operations when concerns arise that call for independent scrutiny. Access to papers and personnel would be needed to discharge these duties, with redaction only for the identity of informants.

1.22 The Commission suggested at paragraph four that the Independent Examiner could also act as an adjudicator to consider requests for information from policing oversight bodies which have been rejected in whole or in part by the police on grounds of national security, and where the oversight bodies wish to appeal that decision. There is a comment that the establishment of the Independent Examiner might also present an opportune time to review the role of the designated judge provided for under section 100 of the Garda Síochána Act 2005[1] and the provisions of part 4 of the Act as they relate to ministerial powers to issue directions regarding access to security material.

1.23 According to the Commission, the Independent Examiner should report to the Taoiseach and should be a part-time appointment. Selecting the right individual for the post would, the Commission felt, be critical. A strong legal background and great credibility within the legal profession would be vital, given the focus of the work on legislation and how it is applied. Excellent communication skills would also be important; the Examiner would need to command public confidence.

1.24 The recommendation of the Commission resulted in the enactment of part 7 of the Policing, Security and Community Safety Act 2024. The legislation enacted reflects to a considerable extent what was envisaged by the Commission but also diverges to a degree. So, while the Commission had envisaged a part-time appointment, the legislation provides that the Independent Examiner role is full-time and eligibility for appointment is confined to those who hold or have held the position of Judge of the High Court, Court of Appeal or Supreme Court.

1.25 It might also be noted that the remit of legislation designated as security legislation extends to crime as well as security matters.

1. The 2005 Act is now repealed and replaced by the Policing, Security and Community Safety Act 2024.

Pre-Establishment

1.26 The Department of Justice, Home Affairs and Migration ("the Department") carried out considerable preparatory work for the establishment of the office of the Independent Examiner of Security Legislation during 2023 and 2024. It included securing a budgetary allocation in the 2025 Estimates, identifying human resource needs and researching IT options for secure methods of drafting, storing and transmitting sensitive material.

1.27 Even prior to my designation, a senior official in the Department had been identified to head up the new office. I met with her shortly after designation. She explained that there was an expectation that a building in the centre of the city on St. Stephen's Green would soon be vacated and this would be the new headquarters for the office of the Independent Examiner. In the meantime, she arranged for me to have the use of a room in the Department, where I read myself into the role. I am grateful to the Secretary General of the Department and her management team for their assistance in that regard. The premises at 87 St Stephen's Green, previously occupied by the Garda Síochána Inspectorate, was made available at the end of November 2024 and I would like to record my appreciation of the cooperation and generosity of the Chief Inspector, Mark Toland, Deputy Chief Inspectors Pauline Shields and Alywin Barton and the Garda Síochána Inspectorate team, who were most accommodating in supporting us in the move.

1.28 In the weeks after designation, a number of staff members were recruited with the support of the human resources team in the Department. The current staff allocation is for six full-time staff members.

1.29 At the time of designation, there was an expectation that establishment day would be in early December 2024. However, for various reasons, there was some slippage in this target date, and the office was formally established on 2 April 2025. The delay in commencement gave the OIE team the opportunity to plan and develop workflows and procedures, put administrative processes in place, provide relevant training opportunities for staff members and develop the corporate identity and branding of the agency. As a result, on establishment day, the office of the Independent Examiner had a live and fully operational website in place, along with documented administrative and governance procedures and an established team already familiar with the work and goals of the organisation.

Activities and Events up to 2 April 2025

1.30 In the intervening period, I undertook further reading with a particular focus on the publications of equivalent agencies, particularly those in the United Kingdom and Australia. During this period, I also embarked on a series of introductory meetings.

1.31 At an early stage, I met with the Garda Commissioner, the Chief of Staff of the Defence Forces, the Police Ombudsman designate, the Chairperson designate and Chief Executive designate of the Policing and Community Safety Authority and with the Director of the National Cyber Security Centre. I also held meetings with senior officials of the Department of the Taoiseach working in the National Security Analysis Centre (NSAC), along with a number of senior officials from different sections of the Department of Justice.

1.32 Somewhat later in the process, I had meetings with the then recently appointed Deputy Commissioner for Security, Strategy and Governance in An Garda Síochána, and with the Assistant Commissioners with responsibility for the Crime and Security Intelligence Service and Organised and Serious Crime. I also held a meeting with the Detective Chief Superintendent in the Security and Intelligence section, who was accompanied by a number of superintendents working under him and each of those at the meeting made a presentation on their work in their respective areas.

1.33 This period also saw meetings with relevant officials of the Revenue Commissioners and of the Competition and Consumer Protection Commission. Both of these bodies have statutory powers which would be subject to oversight by the office when established. I met with the Chief Commissioner and Director of the Irish Human Rights and Equality Commission at their headquarters, and with the Director of Public Prosecutions. During this period, I also met with Judge Dara Hayes, the Complaints Referee under the 1993 Act, the 2009 Act and the 2011 Act, as well as engaging with a predecessor of his in that role. In addition, I met with judges of the High Court who carried out the role of Designated Judge in relation to the various pieces of legislation.

1.34 I spent a morning with the President of the District Court and at his invitation, sat in on a court hearing when he was dealing with applications moved by an inspector of An Garda Síochána seeking court orders under the Communications (Retention of Data) Act 2011.

1.35 On 27 March 2025, I welcomed the Minister for Justice, Home Affairs and Migration ("the Minister"), accompanied by the Secretary General of the Department, to our offices on St. Stephen's Green.

1.36 In addition, I travelled to London and over the course of a day there, I met with my opposite number, the Independent Reviewer of Terrorism and State Threat Legislation, Jonathan Hall KC and two of his predecessors in that role, Sir Max Hill KC and Baron David Anderson of Ipswich KBE KC. I am grateful to all three for their willingness to share their experiences.

1.37 A meeting with Dr. Jonny Byrne, who performs a role similar to mine in Northern Ireland, was scheduled for this period but unfortunately had to be postponed. Subsequently a very productive meeting took place in Belfast. I also met remotely with Jake Blight, the Australian Independent National Security Legislation Monitor.

1.38 During this pre-establishment period, I accepted a number of speaking engagements, including the Annual Dinner of the Mayo Bar Association and one from Probus Dún Laoghaire Marine. On these occasions, my remarks outlined the nature of the statutory office and how I saw my role. I also responded to a request for an extended interview with the security correspondent of a national newspaper.

Post-Establishment

Security Briefings

1.39 Following formal establishment of the organisation, I and my senior staff were given detailed security briefings by An Garda Síochána, the Defence Forces, the Head of the National Security Analysis Centre in the Department of the Taoiseach and the Assistant Secretary with responsibility for Security and Northern Ireland in the Department of Justice, Home Affairs and Migration. This has been of great value in fully understanding the operational and policy context in which the powers provided for in security legislation are utilised.

Planning the Approach to the Review of Security Legislation

1.40 A significant part of the role created for the Independent Examiner of Security Legislation is to take on tasks that had previously been performed by Designated Judges under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1998, the Criminal Justice (Surveillance) Act 2009 and the Communications (Retention of Data) Act 2011, as amended. The operation and effectiveness of these must be reported on annually.

1.41 The other four pieces of legislation must be reported on at least once every three years. At a preliminary stage, I decided to put the Offences against the State Act 1939 at the end of the list for review. While it is arguably the most substantive of the Acts defined as security legislation, my decision was influenced by the fact that the Act had recently been the subject of a review by an expert committee chaired by Mr. Justice Michael Peart, a retired judge of the Court of Appeal, and that decisions arising from that report were pending. The approach decided upon takes account of the fact that the Programme for Government 2025, *Securing Ireland's Future*, commits the Government to considering the report on the Offences against the State Act 1939 and also commits to retaining the Special Criminal Court and annually renewing the provisions of the Offences against the State (Amendment) Act 1998 and the Criminal Justice (Amendment) Act 2009.

1.42 I familiarised myself with the reports of the Designated Judges on the 1993 Act, the 2009 Act and the 2011 Act, as amended. In the past, the practice had been that a judge designated to exercise an oversight role in a particular area would visit the agencies exercising statutory powers in that area on an annual basis.

1.43 From my first engagement with the authorised bodies, I indicated that there would be a significant intensification of the level of oversight, reflecting the establishment of a dedicated office and appointment of a full-time Independent Examiner. While annual review visits had been the norm, it was now the intention that such visits would take place quarterly. Visits would be scheduled so as not to be overly burdensome for these agencies engaged in important work. Visits over and above quarterly visits, including unannounced visits were not excluded. This proposed schedule of quarterly visits was well received by all parties.

1.44 An initial programme of visits to the agencies exercising statutory intrusive powers took place in the period immediately after establishment day. In the six weeks from 29 April to 11 June 2025, I visited An Garda Síochána Headquarters on a number of occasions, interacting with those members of the Security and Intelligence section with responsibilities under the interception, surveillance and data retention legislation; with the Irish Military Intelligence Service of the Defence Forces; with the Revenue Commissioners; with Fiosrú (formerly the Garda Síochána Ombudsman Commission); and interacted with the Competition and Consumer Protection Commission. I also met with the Department of Justice, Home Affairs and Migration in this context.

1.45 In these initial visits, I requested a detailed step-by-step explanation of the procedure followed in the application process, covering multiple hypothetical scenarios. This was most valuable in gaining an understanding of how the implementation of security legislation operates in practice, the procedures, processes and safeguards in place to ensure appropriate assessment

of proportionality and protection of human rights, and the operational challenges that may arise as a result of perceived gaps in the legislation. I also read each of the files that had been opened in relation to applications to exercise statutory powers since the last review visit by Designated Judges and asked questions as needed about the context, operational matters and proportionality test in individual cases.

1.46 In Part Two of this report, I will refer in greater detail to these visits and the individual items of legislation that are required to be reviewed annually. At this stage, I would make some general observations. On every visit, I was made welcome, as were the members of the OIE team who accompanied me. Any questions I posed were answered frankly and comprehensively and where appropriate, were followed up afterwards by supporting material. Each of the visits in this first round involved considerable time spent on questions and teasing out how the internal process would unfold in multiple different situations. On every occasion, the individuals involved were most generous with their time and expertise, for which I am very grateful.

1.47 One aspect that did emerge clearly from the first scheduled series of meetings, was that it was not unusual to see more than one statutory power deployed during the course of an investigation or operation. This is not at all surprising and indeed it is, on reflection, exactly what one would expect to find.

Activity and Engagement

1.48 In addition to the review visits outlined above, post-establishment activity included a number of meetings and participation in conferences and other events. Among these were:

Meetings

- Irish Council for Civil Liberties (ICCL)
- Paul Madden, CT PHARE Project Lead, International Institute for Justice and the Rule of Law (IIJ) (in person and online)
- Financial Intelligence Unit, Garda National Economic Crime Bureau, An Garda Síochána
- Special Detective Unit, An Garda Síochána
- Organised and Serious Crime section, An Garda Síochána
- Banking and Payments Federation Ireland
- Department of Foreign Affairs and Trade, Secretariat to the National Security Authority
- Department of Justice, Home Affairs and Migration, officials from Security and Northern Ireland, Criminal Legislation, Criminal Policy, Justice Service Delivery, Criminal Governance
- Dr Jonny Byrne, Independent Reviewer of the Justice and Security (Northern Ireland) Act 2007
- Bartjan Wegter, EU Counter-Terrorism Coordinator
- Investigatory Powers Commissioner's Office (IPCO) (online and at official level)

Conferences

- IIJ CT PHARE event, "Strengthening Oversight and Accountability of National Security Agencies in South and South-East Asia" (online)
- Working Group on Intelligence and Security Agencies Oversight (IOWG-SSA) launch of the Brussels Memorandum on Good Practices for Oversight and Accountability Mechanisms in Counterterrorism (CT PHARE)
- iTrust 6A Symposium on eEvidence
- Azure Forum for Contemporary Security Strategy
- IHREC Leadership on Human Rights and Equality Conference

Again, during this period, a number of individuals with expertise in these matters came forward to offer me the benefit of their insights and experience. I am grateful to them for this.

PART 2

Review of the Implementation and Effectiveness of Security Legislation

2

Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

Background to the Legislation

2.1 The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 regulates the circumstances in which communications may be lawfully intercepted in the State. While it was the first Act to make explicit provision authorising interceptions, that is not to say that interceptions began with the enactment of the 1993 Act. Rather, it appears that prior to the coming into force of the 1993 Act, warrants providing for the interception of post and telecommunications were issued by the Minister for Justice, but this practice was not underpinned by statute.

2.2 Two decisions, one of the High Court and one of the European Court of Human Rights, formed the backdrop to the legislation. *Kennedy v Ireland* [1987] IR 587[2] arose from the tapping of the phones of two journalists prominent in the political sphere. They then brought proceedings for damages for the unlawful interception of their telephone calls, contending that the actions of State agents amounted to a breach of their personal right to privacy and freedom from unlawful and unwarranted intrusion, which was guaranteed to them by Article 40 of the Constitution.

2.3 The High Court (Hamilton P.) found that the right to privacy, though not specifically guaranteed by the Constitution, was one of the personal rights of the citizen which flowed from the Christian and democratic nature of the State. The Court went on to hold that the constitutional right to privacy included the right to hold private telephone conversations without deliberate, conscious, and unjustified intrusion by servants of the State, and that the right to privacy was not an unqualified right but was subject to the constitutional rights of others and to the requirements of public order, public morality and the common good.

2.4 The decision of the European Court of Human Rights (ECtHR) in *Malone v United Kingdom* (1985) 7 EHRR 14[3] was also of major significance. The ECtHR found that the issuing of warrants on a non-statutory basis for the interception of communications in the UK was in breach of the applicant's right to respect for his private life under Article 8 of the European Convention on Human Rights (ECHR). The Court found that the interference was not "in accordance with law" as required by Article 8(1) because "apart from the simple absence of prohibition [of interception under English law], there would appear to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities."[4]

2.5 The *Malone* judgment gave rise to calls on the UK Government to enact the Interception of Communications Act 1985, legislation which was later found by the Strasbourg court to also not meet the requirements of Article 8 ECHR.[5] Significantly, in the domestic context, the criticisms made by the ECtHR in *Malone*, applied with equal force to the Irish situation.

2. Available at https://ie.vlex.com/vid/kennedy-v-ireland-804355141 [last accessed on 9 April 2026].
3. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57533%22]} [last accessed on 18 March 2026].
4. Note 3, at paragraph 87.
5. See *Liberty v United Kingdom* (2009) 48 EHRR 1. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-87207%22]} [last accessed on 18 March 2026].

2.6 It must be said that while neither in Ireland nor in the neighbouring jurisdiction, was there a statutory basis for interception, that is not to say that the fact of interception was concealed. In *Kennedy*, the State defendants drew attention to section 56 of the Post Office Act 1908 as providing a legal basis for the tapping of the plaintiffs' telephone calls. In the neighbouring jurisdiction, a report of a committee of Privy Councillors, the Birkett Report[6] back in 1957, while commenting that the origin of the power to intercept communications was obscure, pointed to a royal proclamation from 1663, which had outlawed interference with post except under warrant of a Secretary of State.

Statutory Provisions

2.7 Interception is defined in section 1 of the Act as:

> "...an act that consists of the opening or attempted opening of a postal packet addressed to any person, or the delaying or detaining of any such postal packet, or the doing of anything to prevent its due delivery or the authorising, suffering, or permitting of another person (who was not the person to whom the postal packet is addressed) to do so... that, if done otherwise than in pursuance of a direction under section 110 of the Act of 1983, constitutes an offence under section 53 of the Communications Regulation (Postal Services) Act 2011,
>
> or
>
> ...an act that consists of the listening or attempted listening to, or the recording or attempted recording, by any means, in the course of its transmission, of a telecommunications message other than such listening or recording, or such an attempt, where either the person on whose behalf the message is transmitted or the person intended to receive the message has consented to the listening or recording,
>
> and
>
> ...that, if done otherwise than in pursuance of a direction under section 110 of the Act of 1983, constitutes an offence under section 98 of that Act."

The "Act of 1983" referred to above is the Postal and Telecommunications Services Act 1983.

6. *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications* (Cmd. 283, London: HMSO 1957) ("the Birkett Report").

2.8 Postal packets and telecommunication messages are not specifically defined, and instead, there is what might be described as definition by reference in that it is stated that the phrases have the meanings that they have in the Act of 1983, with the addition that it is "for the avoidance of doubt" hereby declared that the phrase "telecommunications message" includes a telegram. The reference to telegrams provides a hint that the legislation is seriously outdated.

2.9 "Serious offence" is defined as an offence which is punishable by a sentence of 5 years imprisonment or more and:

> "(i) that involves loss of human life, serious personal injury or serious loss of or damage to property or a serious risk of any such loss, injury or damage,
> (ii) that results or is likely to result in substantial gain, or
> (iii) the facts and circumstances of which are such as to render it a specially serious case of its kind."

2.10 Section 2(1) makes clear that the Minister for Justice, Home Affairs and Migration may give an authorisation for interception, "but only for the purpose of criminal investigation or in the interests of the security of the State." The rest of section 2 sets out the general requirements for authorisations, including that they shall be given by warrant under the hand of the Minister, in cases of exceptional urgency, they may be given orally, with a requirement on the part of the nominated officer to maintain a record of authorisations (section 2(2)(c)); their time limit of 3 months (section 2(5), which is extendable for further 3 month periods (section 2(6)(a)); and that the Minister may consult the Independent Examiner before deciding whether to give or extend an authorisation. The reference to the Independent Examiner was originally to the Designated Judge.

2.11 There was no such consultation with me during the period under review, and I am not aware that there has been such a consultation with a Designated Judge in the past.

2.12 Sections 4 and 5 detail the conditions which the Minister must consider fulfilled before issuing an authorisation. Section 4 deals with criminal investigations and section 5 with situations involving the security of the State.

2.13 Section 4(a)(i) provides that the conditions are:

> "that –
>
> (I) investigations are being carried out by the Garda Síochána, the Police Ombudsman or another public authority charged with the investigation of offences [whether already committed, suspected or apprehended[7]] of the kind in question, concerning a serious offence or a suspected serious offence,
> (II) investigations not involving interception have failed, or are likely to fail, to produce, or to produce sufficiently quickly, either or, as the case may be, both of the following, that is to say:
> (A) information such as to show whether the offence has been committed or as to the facts relating to it,
> (B) evidence for the purpose of criminal proceedings in relation to the offence,
> and
> (III) there is a reasonable prospect that the interception of postal packets sent to a particular postal address or of telecommunications messages sent to or from a particular telecommunications address would be of material assistance (by itself or in conjunction with other information or evidence) in providing information, or evidence, such as aforesaid…
>
> …and
>
> (b) that the importance of obtaining the information or evidence concerned is, having regard to all the circumstances and notwithstanding the importance of preserving the privacy of postal packets and telecommunications messages, sufficient to justify the interception."

7. Section 4(a)(ii) of the 1993 Act. Apprehended offences were added by section 12(b) of the Garda Síochána (Amendment) Act 2015.

2.14 Section 5 sets out the conditions applicable to interceptions in the interests of the security of the State:

> "(a) that there are reasonable grounds for believing that particular activities that are endangering or likely to endanger the security of the State are being carried on or are proposed to be carried on,
>
> (b) that investigations are being carried out by or on behalf of the person applying for the authorisation concerned to ascertain whether activities of the kind aforesaid are in fact being carried on or proposed to be carried on and, if so, by whom and their nature and extent,
>
> (c) that investigations not involving interception have failed, or are likely to fail, to produce, or to produce sufficiently quickly, information that would show whether the activities are being carried on or proposed to be carried on and, if so, by whom and their nature and extent,
>
> (d) that there is a reasonable prospect that the interception of postal packets sent to a particular postal address or of telecommunications messages sent to or from a particular telecommunications address would be of material assistance (by itself or in conjunction with other information) in providing information such as aforesaid, and
>
> (e) that the importance of obtaining the information concerned is, having regard to all the circumstances and notwithstanding the importance of preserving the privacy of postal packets and telecommunications messages, sufficient to justify the interception."

2.15 Section 6 deals with the procedures for applying for an authorisation. It requires that an application must be made by the Garda Commissioner or the Police Ombudsman in cases of criminal investigation, or by either the Garda Commissioner or the Chief of Staff of the Defence Forces in cases involving the security of the State. Applications are required to be in writing to a nominated officer of the Minister and must include sufficient information to enable the Minister to determine whether the conditions prescribed by section 4 or section 5 have been met. If application is 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.

2.16 Section 6(2) relates to the role of the nominated officer of the Minister. The officer, invariably a very senior official of the Department of Justice, Home Affairs and Migration, is required to consider applications under the section and having made any enquiries he or she thinks necessary, makes a signed submission to the Minister stating an opinion as to whether or not the conditions specified in section 4 or 5, as the case may be, of the Act stand fulfilled in relation to the proposed interception. If the nominated officer is of the opinion that those conditions do not stand so fulfilled, he or she states in what respects they do not so stand.

2.17 Interestingly, section 6(3) states that information in the possession of the nominated officer, whether as a result of a previous authorisation, application or otherwise, may be treated as if it had been included in the application.

2.18 There is provision for the role of the nominated officer to be performed by another official in the absence of the nominated officer.

2.19 Section 7 provides for interceptions ceasing to be in force when no longer required.

2.20 Section 8 deals with the role of the Independent Examiner to ascertain whether provisions of the Act are complied with and to keep the operation of the Act under review. Section 8(6) provides that if the Independent Examiner informs the Minister that he or she considers that a particular authorisation that is in force should not have been given or should be cancelled or should not have been renewed, the Minister is required to inform the Minister for Climate, Energy and Environment and to then cancel the authorisation. This situation has not occurred since my appointment.

Complaints Procedure

2.21 Section 9 provides for a complaints procedure and creates the office of Complaints Referee. If, following an investigation into a complaint, the Complaints Referee finds that there has been a breach of the provisions of the Act, he or she must notify the complainant and report the finding to the Taoiseach. The Complaints Referee can quash the authorisation and can order the destruction of any copy of the intercepted communication and there is also provision for recommending the payment of compensation to the complainant.

2.22 Where the Complaints Referee has found that there was not a breach of specified provisions of the Act but has come to the view that the offence was not a serious one as defined, he or she may refer the question of the seriousness of the offence to the Independent Examiner. If the Independent Examiner agrees that the offence was not serious, then the same procedures as set out above arise; that is to say, notifying the complainant, reporting to the Taoiseach, the power to quash, to order destruction, to recommend compensation and so on. If the Independent Examiner comes to the view that the offence was a serious offence, then the Complaints Referee is required to notify the complainant that there has been no contravention of the Act.

2.23 This requirement to notify the complainant of the fact that there has been no contravention and to go no further than that may be seen as an application of the principle of "neither confirming nor denying."

2.24 The office created by this section has, as we will see, been allocated a role with the same function under the 2009 and 2011 Acts.

2.25 Section 10 deals with certain proceedings and evidence. Three things strike me as noteworthy:

- The consent of the DPP is required for prosecutions of unlawful interception offences under specified postal and telecommunications legislation (section 10(1)(a));
- In any such prosecution, the factual question of whether an act or omission potentially attracting criminal liability actually occurred, must be determined before any evidence is adduced as to whether an authorisation was given (section 10(2)(b));
- Outside of the context of such proceedings, no person is compellable to give evidence that would tend to show that an authorisation was given or applied for, before any court, tribunal or person other than the Independent Examiner or the Complaints Referee (section 10(3)).

2.26 Hogan, Morgan and Daly suggest that the constitutionality of this subsection might be in question on the basis of the Supreme Court judgment in *Ambiorix Ltd v Minister for the Environment (No. 1)* [1992] 1 IR 277[8]:

> "In defence of such a safeguard, it is said that any person 'wanting to find out whether his telephone had been tapped' might start proceedings with a view to compelling an official 'to say whether there had been an interception' [quoting the then Minister for Justice, Pádraig Flynn, explaining the rationale for the provision in the Dáil]. Nevertheless, while the public interest in protecting the integrity of an official interception system must be very great, the constitutionality of such a far-reaching exclusion clause must, in the light of cases such as *Murphy* and *Ambiorix*, be open to question. In addition, without the benefit of discovery, a plaintiff who was the victim of an unlawful interception could not easily establish this fact. Here is the very type of 'Catch-22' situation which, as we have already seen, was stigmatised by McCarthy J. in *Ambiorix* as a breach of fair procedures."[9]

As we will see in due course, a somewhat more nuanced approach has been taken in the Criminal Justice (Surveillance) Act 2009.

8. Available at https://ie.vlex.com/vid/ambiorix-ltd-v-minister-802625257 [last accessed 18 March 2026].
9. *Administrative Law in Ireland* (5th ed., Round Hall 2019) at paragraph 22-136.

2.27 Section 12 imposes obligations on the Minister to disclose to the minimum extent necessary both the fact of and the content of authorised interceptions, and to ensure that copies of communications are not made unnecessarily and are destroyed when no longer necessary. Necessary is defined in terms of the prevention or detection of serious offences or in the interests of State security.

2.28 Sections 13 and 14 amend and repeal other legislation. Of particular note is the repeal of section 18 of the Official Secrets Act 1963. This gave the Minister power to require the production of certain telegrams. This is of interest as section 18 was a rare example of a legislative power to access a particular form of communication before the 1993 Act.

Review Visits

An Garda Síochána

2.29 My first review visit to An Garda Síochána came against the background of having engaged in earlier meetings with the Commissioner and his colleagues, including the Deputy Commissioner in charge of Security, Strategy and Governance following his appointment to that rank, and the Assistant Commissioners with responsibility for the Crime and Security Intelligence Service and for Organised and Serious Crime.

2.30 It also followed a meeting in my office with the relevant Security and Intelligence Detective Chief Superintendent, who was accompanied by the various superintendents who make up his team. Each of the superintendents provided a presentation in relation to their work. The members of these Security and Intelligence teams work in particular areas involving a specific statutory power, be that lawful interception, surveillance or data retention. I commented earlier on the fact that this meeting gave me a very clear picture of the context in which statutory powers are used by An Garda Síochána.

Procedure

2.31 Resort to lawful interception of postal packets or telecommunications is centralised. All activity in this area is dealt with by a unit within the Security and Intelligence section of An Garda Síochána based at Garda Headquarters. This is the same unit that deals with data retention on a day-to-day basis.

2.32 Where a view is formed within An Garda Síochána at a divisional or district level that assistance by way of additional intelligence is necessary to advance serious criminal investigation or is in the interests of safeguarding the security of the State, an application is made to the relevant team in Security and Intelligence, either on the criminal intelligence or national security intelligence side, as appropriate. All requests are funnelled through these channels, and this is viewed as being extremely important in terms of both internal quality control and the desirability of maintaining a separation between the investigative team and those applying for authorisations.

2.33 When the application is then submitted to the unit within Security and Intelligence, it is assessed at detective sergeant level to ascertain if there is enough substance to meet the statutory threshold and whether the application is feasible. Frequently, clarification or further information will be requested. After that initial assessment, the application then goes up the line for consideration by an inspector and then to a superintendent. At that stage, a draft application addressed to an operator or service provider is drawn up. However, before it can be acted upon, it must be approved by the Detective Chief Superintendent, and the matter is then submitted to the Garda Commissioner for personal consideration. The view is taken within An Garda Síochána that a so-called "wet signature" – a traditional, physical signature in hard copy – is required from the Commissioner. It is also considered that the Commissioner can only delegate functions under the Act if absent from duty or on annual leave. This interpretation can be problematic if the Commissioner is out of the jurisdiction on official business, for example, attending a cross-border meeting, international meetings with partner police and security agencies, or other EU or international engagements. Only when the request for authorisation has been signed by the Commissioner, can the matter be submitted to the nominated officer of the Minister.

2.34 The procedure followed in the case of authorisations sought in furtherance of a criminal investigation and authorisations sought to support the security of the State are essentially the same. If the authorisation is approved, it is kept under constant review in terms of proportionality. In addition to the ongoing review, there is a more formal internal review every 14 days, and the question of whether the interception is still required, is still justified, and continues to be proportionate is considered, having regard to the importance of respecting privacy of communication. This represents a further safeguard and is to be commended.

2.35 An authorisation is valid for three months from when it is issued and there is provision for renewal. Typically, interceptions authorised in the interests of the security of the State tend to be of longer duration than those issued in furtherance of a criminal investigation. This same pattern is also true in relation to the exercise of powers under the 2009 Act. This explanation is a simple one – that threats to the security of the State tend to be long term or at least medium term.

2.36 On my first oversight visit, I read the files relating to all authorisations since 2 April 2025, the date of establishment of the office. The opportunity to read every new file and ask questions about each use of the statutory powers has given me a comprehensive picture of the use of interception by An Garda Síochána and the level of consideration and test of proportionality applied in all cases.

2.37 On the basis of consideration of all relevant files on the three rounds of review visits, and the conversations that I had on each occasion with members of An Garda Síochána involved in the operation of the 1993 Act, I am satisfied that the Act is operated by An Garda Síochána in a responsible and professional manner.

2.38 The ability to intercept communications in appropriate circumstances and subject to appropriate safeguards is important, both for investigating and preventing serious crime and the interest of the security of the State. I was satisfied that all applications for authorisation received careful consideration when received by Security and Intelligence. The fact the members of the Security and Intelligence team managing the application process are not themselves involved in the investigation, but are responding to requests from investigators, contributes to effective internal control. There is a clear dividing line between the roles played by applicant investigators and the authorising team at Garda Headquarters.

2.39 On foot of my conversations with the senior members of the unit engaged with the 1993 Act and my examination of the files, I am fully satisfied that there is no rubber stamping of requests. The process requires that all particulars of a request are fully laid out – for example, the strategic goal of the use of interception in a particular investigation, why this level of intrusion would be the only feasible way of gaining the intelligence sought, what other methods of investigation had already been deployed – and the application is then thoroughly assessed in terms of proportionality, relevance and necessity. It should indeed be noted that in the period examined, 10% of applications were sent back for clarification or further information and the internal refusal rate was 35% of all applications. This appears to me to be a clear indication that all applications are thoroughly assessed to ensure that the appropriate threshold is met.

The Defence Forces

2.40 My first review visit to the Defence Forces took place in the new headquarters of the Irish Military Intelligence Service (IMIS). It came against a background of earlier interaction, which involved a meeting with the then Chief of Staff, who was accompanied by a senior officer in IMIS, as well as a preliminary meeting with the Director of Military Intelligence and his deputy.

2.41 As with An Garda Síochána, resort by the Defence Forces to their statutory powers under the 1993 Act is centralised. A similar approach is taken by the Defence Forces when resorting to their other statutory powers that were the subject of oversight by a Designated Judge, which now fall within the remit of the Independent Examiner.

Procedure

2.42 The procedure followed by IMIS to govern the use of interception powers and indeed, the other statutory powers that are subject to oversight, differs slightly from the approach taken by An Garda Síochána. In the case of the Defence Forces, officers and members are assigned to work in a particular area of concern, for example, the internal security of the Defence Forces, rather than the exercise of a specific statutory power. The assigned person leading the team dealing with a particular area is referred to as a desk officer. Desk officers might on occasion find themselves addressing the question of whether to move towards seeking to invoke statutory powers and if in that situation, having to make a judgement as to which would be the most appropriate statutory power.

2.43 The procedures within the unit require that before the proposed application for a telecommunications or postal interception is submitted to the Chief of Staff, the application is considered within the section by no fewer than three officers of different rank. Each officer addresses his or her mind to the threat to the security of the State and the necessity for the proposed interception, what results are to be expected, and the proportionality of the proposed interception, weighed against the value of privacy of postal and telecommunications. The question of collateral intrusion into privacy rights is also considered.

2.44 On the occasion of my first review visit, the early part involved presentations by a number of the desk officers, each of whom outlined their particular areas of responsibility. In the course of these presentations, there were specific references to occasions on which each of the statutory powers, including that of interception, had been invoked. It was explained how significant the availability of the powers had been and how in these particular cases, resort to the powers had resulted in successful outcomes.

2.45 This visit also involved my reading each of the new files opened since the establishment of my office, along with ongoing current files. On subsequent visits, I read the files relevant to the period since the previous visit.

2.46 As a result of my conversations and my reading of the files, I am fully satisfied that the legislation is being operated by IMIS in a conscientious, responsible and careful manner. Any questions that I had while reading the files were dealt with comprehensively and to my satisfaction.

Fiosrú

2.47 The Police Ombudsman now has powers under this legislation. Provision in this regard is made by section 274(1)(d) of the Policing, Security and Community Safety Act 2024 amending the 1993 Act. In all of my interactions with Fiosrú, we discussed this legislative provision. However, the focus of the discussions centred on the exercise of other statutory powers which were under review. During the review period, the Police Ombudsman did not exercise the statutory powers provided for under the 1993 Act.

The Department of Justice, Home Affairs and Migration

2.48 In the course of each round of visits, I met with the officials of the Department of Justice, Home Affairs and Migration with responsibilities under the 1993 Act. On each occasion, I discussed with them their sense of recent trends and developments. Each of these meetings was attended by the Minister's nominated officer, along with an official designated to substitute for that officer when required.

2.49 At the first of these meetings, the procedure that was followed on receipt of an application for an authorisation was set out for me in detail. In particular, it was explained that frequently, on receipt of an application, there would be contact between the nominated officer and the applicant to seek clarification or further information. On these visits I read files the Department held relating to applications for authorisations since establishment day of the office or since the previous visit.

2.50 Overall, I was fully satisfied that the procedures in place are comprehensive and thorough and that no application for authorisation is presented by the nominated officer to the Minister for consideration and decision without having undergone an appropriate level of scrutiny and examination.

Incidence of Use of Statutory Powers

2.51 I have considered whether to provide statistics as to the number of occasions when the interception power was utilised. However, after having given the matter some thought, I have concluded that it would not be appropriate to do so. I have come to this view for a number of reasons. Overall figures would be of little value, and their publication might be misleading. In some instances, figures that might be provided could be distorted by the fact that there may be multiple authorisations in respect of the same phone or the same person of interest. This can occur when the individual using the targeted phone changes network or where it is unknown or uncertain which is the relevant network, in which case, authorisations must be sent to all network providers.

2.52 Overall, I can say that the level of interception is broadly consistent with what has been reported on for a number of years. In the case of the Defence Forces, there has been some reduction in the extent of resort to the intrusive power in recent times, though predating the period under review, and cogent reasons were provided for this.

2.53 Certainly, the level of interception can fairly be described as modest. The overall level does not offer any support whatsoever for any suggestion that the bodies vested with powers in this area have exercised them in a cavalier fashion. On the contrary, the volume of requests for authorisation by those bodies which had actually exercised them during the period under review, speaks volumes as to a restrained and focused invocation of statutory powers.

2.54 That impression was reinforced when it came to the consideration of the contents of individual files. Without exception, the rationale for the application and the justification for interception emerged clearly from each of the files.

Observations in Relation to the 1993 Act and Associated Recommendations

Gaps

2.55 The fact that the 1993 Act is seriously out of date has been commented on publicly by a number of the holders of the office of Designated Judge in the course of annual reports.

2.56 There are number of areas in which the legislation is deficient. In this section, I intend to highlight gaps that have become apparent to me during my review visits:

- The most significant arises from 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 Service). The Act makes no provision for the interception of data-based or over-the-top (OTT) services. Examples of OTT services are WhatsApp, Telegram and Snapchat, to mention just a few. There is no legislative basis to access the content of data-based material, such as webpages or internet browsing history through interception. This has the potential to impinge on the State's ability to fulfil its obligations under Part 3 of the Criminal Justice (Mutual Assistance) Act 2008.
- The use of electronic scanning equipment designed to locate and record identifier data from mobile devices is permitted in many other jurisdictions. A common example of such equipment is the IMSI (International Mobile Subscriber Identity) catcher. IMSI catchers are telephone eavesdropping devices used for intercepting mobile phone traffic and tracking location data. They operate by acting as decoy mobile phone towers and can support an investigation by identifying potential linked targets or devices of interest. Their use is sometimes referred to as "man in the middle"[10] attacks. Legislation should be developed to provide for the use of these and other electronic scanning equipment designed to locate and record identifier data.
- In relation to postal interceptions, the legislation only covers An Post and not couriers or other delivery services.

2.57 I recommend that these gaps in coverage should be addressed and note that the Minister, in a public statement on 20 January 2026[11], indicated that he had secured Government approval to draft the heads of a bill to govern the lawful interception of communications, which will replace the 1993 Act.

Encryption

2.58 Encryption has been described as "the turning of information that is in an intelligible form – usually described as 'plaintext' – into information which is not – usually described as 'ciphertext'".[12] Ciphertext is made up of an unreadable string of letters, numbers and symbols. Information may be encrypted "in transit", as it moves between electronic devices, or "at rest", as it is stored in a device.

2.59 OTT apps now offer "end-to-end" encryption (abbreviated to "E2EE") as standard, meaning that the plaintext is encrypted by the sender's device using an encryption key and is only decrypted once it reaches the receiver's device using another decryption key. As a result, the communications service provider responsible for transmitting the message, and anyone else who

10. See Paul F Scott, "Secrecy and surveillance: lessons from the law of IMSI catchers" (2019) 33(3) *International Review of Law, Computers & Technology* 349, 352. Available at https://eprints.gla.ac.uk/177707/7/177707.pdf [last accessed on 18 March 2026].
11. Press release, Department of Justice, Home Affairs and Migration: Minister Jim O'Callaghan strengthens lawful interception powers. Available at https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/press-releases/minister-jim-ocallaghan-strengthens-lawful-interception-powers/ [last accessed on 18 March 2026].
12. Paul F. Scott and Micheál Ó Floinn, "Technical backdoors and legal backdoors: regulating encryption in the UK" (2024) 35(3) *King's LJ* 441, 442. Available at https://eprints.gla.ac.uk/343679/1/343679.pdf [last accessed on 18 March 2026].

intercepts the message in transit, only has access to the unintelligible ciphertext of the message, not the intelligible plaintext. By using E2EE, only the sender and receiver of the message – the "end users" – are able to read the plaintext message.

2.60 The question of encryption poses difficult challenges. On the one hand, very many people in many different walks of life on a daily basis use encryption and are encouraged to do so. It has brought significant additional security to financial transactions and communications.

2.61 However, encryption holds equal attraction for criminals and terrorists. Although the technology is becoming increasingly sophisticated, law enforcement has recorded some notable successes such as in the case of EncroChat, where a communications network favoured by criminals was infiltrated by French and Dutch authorities.

2.62 The Minister's statement makes clear that it is his view that communications from all devices, whether encrypted or not, should be capable of being lawfully accessed. It is almost impossible to argue that criminals or terrorists should enjoy immunity from having their communications accessed. However, legislation to achieve that while protecting the privacy rights of everybody else will not be easy. Certainly, clear and robust safeguards will be required.

Storage and Access

2.63 The Act does not deal specifically with the issue of retention, secure storage, and access to the product of interception. More modern legislation in the area of intrusive powers such as the Criminal Justice (Surveillance) Act 2009 imposes specific obligations in this regard, and indeed provides for the making of Ministerial orders setting out greater detail. While I am quite satisfied that the agencies exercising powers in this area are fully aware of the importance of secure storage and restricting access, it is an issue that should be addressed in amending legislation.

Situations of Urgency

2.64 The procedure that must be followed before authorisation is issued by the Minister is a complex one, involving the Garda Commissioner, a nominated departmental official and the Minister for Justice, Home Affairs and Migration. In the case of authorisations sought in support of safeguarding the security of the State by the Defence Forces, there is an involvement by the Chief of Staff and the Minister for Defence, as well as the Minister for Justice, Home Affairs and Migration. At present, the only provision made to address a situation of urgency is that ministerial authorisations, which are usually in writing, may be given orally in cases of exceptional urgency. Other legislation in the security area such as the Criminal Justice (Surveillance) Act 2009 and the Communications (Retention of Data) Act 2011, make provision for situations of urgency. There should be provision for a simplified and accelerated procedure in cases of urgency, with a requirement for authorisations to be reported on as soon as practical and retrospective authorisation obtained.

2.65 The apparent requirement for a physical signature or "wet signature" from the Garda Commissioner and the difficulties that this can present if he is abroad on business should be addressed.

Applications for Authorisations

2.66 The provisions in relation to prior authorisation for interception of telecommunications and postal packets diverge in a number of respects from the regimes that have been put in place for authorisations to resort to other statutory powers, in particular under the Criminal Justice (Surveillance) Act 2009 and the Communications (Data Retention) Act 2011. In the case of interception, lawful interception requires that an authorisation be issued by the Minister for Justice, Home Affairs and Migration. There is at present no role for prior judicial or other independent consideration, save for a provision at section 2(7) which has rarely, if ever, been used, that the Minister may consult the Independent Examiner, previously the Designated Judge, when considering whether to grant or extend a particular application. There is provision for a concerned individual to make a complaint to the Complaints Referee.

2.67 As far as the other statutory powers are concerned, in the case of surveillance, a distinction is drawn between tracking devices and more intrusive surveillance devices, with the latter only being permitted to be deployed on foot of a warrant issued by a judge of the District Court. Of note is that the 2009 Act also makes provision for an expedited procedure in circumstances of urgency with provision for a subsequent application for judicial affirmation.

2.68 Likewise, in the case of data retention, the legislation distinguishes between different kinds of data with different procedures for seeking authorisation applicable. In the case of more sensitive data, as we will see in the section in this report dealing with the 2011 Act, the authorisation procedure involves application to a judge.

2.69 The fact that the 1993 Act makes no provision for judicial and very limited provision for independent involvement at the application for authorisation stage is not consistent with the approach taken in the other more recent statutes making provision for the exercise of intrusive powers on a statutory basis.

2.70 A survey of the approach taken in a large number of different jurisdictions by the Venice Commission, entitled *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware*[13] and adopted by the Venice Commission at its 141st plenary session in Venice in December 2024 suggests that the absence of judicial or other independent authorisation means that the Irish approach is something of an outlier.

2.71 The jurisprudence of the European Court of Human Rights, including in decisions such as *Szabó and Vissy v Hungary* (2016) 63 EHRR 3,[14] while not perhaps overly prescriptive, would seem to favour prior independent authorisation.

2.72 From the early days post designation, in the course of engagements with various stakeholders, I indicated that I was at least open to the idea of moving to a degree of judicial or other independent involvement. I did not receive any pushback, but I would stress that I was not focusing on any particular model but simply identifying a possible direction of travel. If there is to be movement away from the executive having an exclusive role in the area of authorisation to one where a judicial or other independent authority either substitutes for that role or augments it, the first question is whether the role should be allocated to a judge or to some other independent authority. I have no doubt that as a matter of practicality, judicial authorisation is preferable.

2.73 The number of applications requiring consideration in a particular year is likely, based on past experience, to be modest and would not justify the establishment of a new office such as that of a dedicated authorising commissioner. That is even more clearly the case if the view were taken that if there were to be a new structure, it would be necessary to extend powers to authorise to more than one individual in order to allow for situations which would inevitably arise where a single individual might be unavailable.

2.74 On the other hand, if a role in the authorisation process is to be entrusted to judges, this would complement the role played by them in considering applications for authorisations under other security legislation and would also complement their long-established role in considering applications for warrants across a wide range of areas.

2.75 I note that the statement by the Minister refers to the fact that he has responsibility at present under the 1993 Act for authorising interceptions and that the general scheme of the bill which is being prepared will maintain a role for the Minister but will also introduce judicial authorisation of interception requests for the first time.

2.76 If there is to be a role for prior judicial authorisation, and it would appear that there is broad support for that, there are several different ways in which that could be achieved. One would be to simply transfer the powers now exercised by the Minister to a judge of the District Court. Another possibility would be to provide for a dual lock, which would require applications to be approved by the Minister and by a judge. This, it might be noted, is an approach that has found favour in the United Kingdom.

13. Available at https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e [last accessed on 18 March 2026].

14. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]} [last accessed on 18 March 2026].

2.77 Another possibility would be to distinguish between authorisations sought in the course of criminal investigations and those sought on grounds of State security. This might see applications on the criminal side being dealt with by judges and those where the application is sought on grounds of the security of the State being considered by the Minister, either alone or alongside a judge as part of a dual lock approach.

2.78 If the Minister is to have a continuing role in authorisations, it is probably because the view is taken that where the question of State security is in issue, that there should be an involvement by the Minister for Justice, Home Affairs and Migration. While I see the force of that argument, I am not fully convinced. When other intrusive statutory powers are being considered by reason of State security, authorisations happen without ministerial involvement. Why should interception be different? While of course it is entirely appropriate that the Minister should be fully apprised of all significant developments in the area of State security, it does not seem necessary to me that this should be at the level of whether a particular individual phone or postal packet should be intercepted.

2.79 While arguments could be made for any of the options to which I have referred and probably for others as well, and all represent movement in the same direction, it seems to me that the neatest approach is to simply entrust the task of prior authorisation to the judiciary and this, on balance, is the approach I would favour.

Jurisprudence of the ECtHR

2.80 In the area of interception of communications, the ECtHR has consistently emphasised the need for regulation and supervision and has insisted that the law should specify with clarity the manner in which the right to privacy can be interfered with by state authorities:

- The law must be sufficiently clear in its terms "to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to conduct surveillance."[15]
- Domestic law governing these investigative measures must be accessible and compatible with the rule of law.[16] In this regard, an individual must be able to foresee the implications of the legislative measures and they must be adequately clear to give citizens an indication as to the circumstances and conditions in which public authorities are permitted to resort to measures of surveillance and interception of communications.[17]
- The discretion vested in the State to authorise interception and surveillance cannot be an unfettered power and the scope and manner of such discretion must be clearly indicated. This includes a requirement for "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using, and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed".[18]

This jurisprudence will need to be in the forefront of the minds of those preparing legislation in this area.

15. *Malone v United Kingdom* (1985) 7 EHRR 14, at paragraph 67. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57533%22]} [last accessed on 18 March 2026].
16. *Liberty v United Kingdom* (2009) 48 EHRR 1. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-87207%22]} [last accessed on 18 March 2026]; *Malone v United Kingdom* (1985) 7 EHRR 14, at paragraph 68.
17. *Weber and Saravia v Germany* (2008) 46 EHRR SE5, at paragraph 93. Available at https://hudoc.echr.coe.int/eng#{%22appno%22:[%2254934/00%22],%22itemid%22:[%22001-76586%22]} [last accessed on 18 March 2026].
18. *Weber and Saravia v Germany* (2008) 46 EHRR SE5, at paragraphs 94-5.

SUMMARY OF RECOMMENDATIONS – 1993 ACT

- Develop legislative basis for interception of and access to modern, digital communications.
- Provide legislative basis for lawful access to all communications, including encrypted communications, incorporating appropriate safeguards.
- Provide for secure storage and access in any amending or new legislation.
- Develop legislative basis for use of electronic scanning equipment that can locate and record identifier data from mobile devices.
- Broaden the scope of postal interception to include delivery and courier services beyond An Post.
- Develop an accelerated procedure to provide for situations of urgency.
- Address the apparent need for the Garda Commissioner to provide a physical signature.
- Examine potential models for prior judicial authorisation of interception applications.

3

Criminal Justice (Surveillance) Act 2009

Background to the Legislation

3.1 The backdrop to the legislation was significant public concern at the time in relation to what appeared to be a dramatic increase in organised crime. This is apparent in the repeated references to it in the Oireachtas debates. In introducing the Criminal Justice (Surveillance) Bill 2009 to the Dáil, 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."[19]

3.2 At an early point in her judgment in *The People (Director of Public Prosecutions) v Hannaway* [2021] IESC 31, [2023] 2 IR 591,[20] O'Malley J. commented that while the appeal that was before the Court was concerned with the exercise of power for the purpose of criminal investigation, it should be noted that the statute also clearly contemplates the gathering of information for intelligence purposes.

Statutory Provisions

3.3 Despite the broad and open-ended title, and indeed, long title of the legislation, the remit of the 2009 Act is more confined than might at first appear, with much surveillance activity falling outside its scope.

Surveillance is defined in section 1 of the Act as:

> "(a) monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or
>
> (b) monitoring or making a recording of places or things
>
> by or with the assistance of surveillance devices."

A surveillance device is defined in the same section as:

> "…an apparatus designed or adapted for use in surveillance, but does not include—
>
> (a) an apparatus designed to enhance visual acuity or night vision, to the extent to which it is not used to make a recording of any person who, or any place or thing that, is being monitored or observed,
>
> (b) a CCTV within the meaning of section 38 of the Garda Síochána Act 2005, or
>
> (c) a camera (including a video camera), to the extent to which it is used to take photographs or video footage of any person who, or any thing that, is in a place to which the public have access."

3.4 Section 1 also provides a definition of a tracking device as meaning a "surveillance device that is used only for the purpose of providing information regarding the location of a person, vehicle or thing."

19. Dáil debate 29 April 2009, vol 681, no 2. Available at https://debatesarchive.oireachtas.ie/debates%20authoring/debateswebpackpre2016.nsf/takes/dail2009042900010?opendocument [last accessed 18 March 2026].
20. Available at https://ie.vlex.com/vid/the-people-at-the-866550641 [last accessed on 18 March 2026].

3.5 The phrase "by or with the assistance of surveillance devices" in the definition of surveillance is key. It means that covert, or indeed overt surveillance involving following or observation without the deployment of a surveillance device falls outside statutory regulation.

3.6 The somewhat restricted statutory definition in this jurisdiction may be contrasted with the approach taken in the United Kingdom. There, surveillance is defined in section 48(2) of the Regulation of Investigatory Powers Act 2000 as including:

> "(a) monitoring, observing or listening to persons, their movements, their conversations or 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."

3.7 It might be noted that the definition is not exhaustive, and that the monitoring, observing or listening does not have to be recorded, and does not have to involve the use of technology in order to come within the statutory definition in the UK.

3.8 Surveillance, other than in a statutory context, was considered by the High Court and Supreme Court in the case of *Kane v Governor of Mountjoy Prison* [1988] 1 IR 757.[21] The background to the case is that Mr. Kane had been found hiding in the attic of a house close to where firearms and ammunition were located. He was arrested and detained under section 30 of the Offences against the State Act 1939 and at the end of the 48-hour period, was released from custody. However, on his release he was subject to intense overt surveillance by members of An Garda Síochána. He was followed by gardaí wherever he went, which included a high-speed chase. When the car in which Mr. Kane was travelling was eventually stopped, he was rearrested, the grounds being that he had allegedly assaulted a member of the gardaí.

3.9 Whilst Mr. Kane was in custody in relation to the assault matter, gardaí obtained a provisional warrant pursuant to section 49 of the Extradition Act 1965. When released on bail in relation to the assault charge, he was arrested in execution of the provisional extradition warrant, brought before the District Court and remanded in custody. Mr. Kane sought his release under Article 40 of the Constitution, contending that the extent and nature of the surveillance conducted by gardaí amounted in law to unlawful continuance of his detention after the expiry of 48 hours. He also contended that the surveillance amounted to unlawful harassment and that it constituted an infringement of his constitutional right to privacy and freedom of movement. In rejecting the application, both the High Court and the Supreme Court laid emphasis on the fact that while Mr. Kane was subject to very intensive overt surveillance, he was not prevented from going to where he wanted to go, so the surveillance, intensive as it was, could not be regarded as a form of de facto detention.

3.10 The Act applies to surveillance carried out by members of An Garda Síochána, designated officers of the Police Ombudsman (initially provided for by section 13(b) of the Garda Síochána (Amendment) Act 2015 and now by section 281(d) of the 2024 Act amending the 2009 Act) members of the Defence Forces, officers of the Revenue Commissioners and authorised officers of the Competition and Consumer Protection Commission, provided for by the Competition (Amendment) Act 2022.

3.11 The Act as amended provides that a member of the Garda Síochána, a member of the Defence Forces, an officer of the Revenue Commissioners, a designated officer of the Police Ombudsman or an authorised officer of the Competition and Consumer Protection Commission shall carry out surveillance only in accordance with a valid authorisation or an approval granted in accordance with sections 7 or 8.

3.12 Section 4 of the Act deals with applications for authorisation. It provides a superior officer of An Garda Síochána, defined in statute as not below the rank of superintendent, may apply to a District Court judge for an authorisation where he or she has reasonable grounds for believing that:

21. Available at https://ie.vlex.com/vid/kane-v-governor-of-792894597 [last accessed on 18 March 2026].

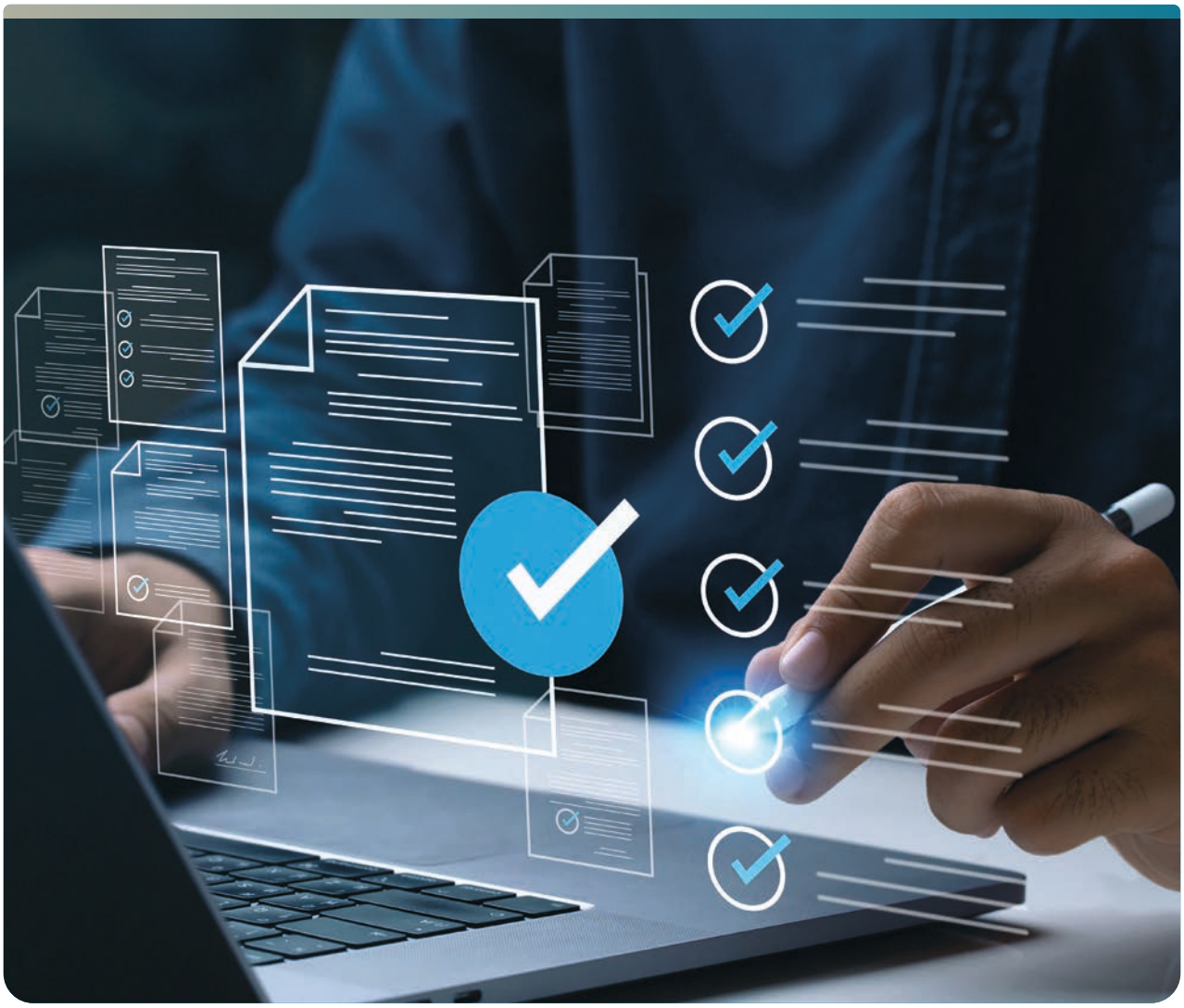
"(a) as part of an operation or investigation being conducted by the Garda Síochána concerning an arrestable offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence,

(b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of arrestable offences, or

(c) the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State."

3.13 Similarly, the Act provides that a superior officer of the Police Ombudsman, defined as a senior designated officer, may apply to a judge of the District Court for an authorisation where he or she has reasonable grounds for believing that as part of an investigation being conducted by the Police Ombudsman concerning an arrestable offence, the surveillance sought to be authorised is necessary for the purpose of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence.

3.14 Again, the Act provides that a superior officer of the Defence Forces, defined as not below the rank of colonel may apply to a judge of 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.



3.15 Likewise, a superior officer of the Revenue Commissioners, defined as an officer not below the rank of principal officer, may apply to a judge of the District Court for an authorisation where he or she has reasonable grounds for believing that:

> "(a) as part of an operation or investigation being conducted by the Revenue Commissioners concerning a revenue offence, the surveillance being sought to be authorised is necessary for the purpose of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purpose of proceedings in relation to the offence, or
>
> (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of revenue offences."

The term "revenue offence" is defined in the interpretation section of the statute.[22]

3.16 The Act also provides that a superior officer of the Competition and Consumer Protection Commission, again defined as not below the rank of principal officer, may apply to a judge of the District Court for an authorisation where he or she has reasonable grounds to believe that as part of an investigation being conducted by the Competition and Consumer Protection Commission concerning a relevant competition offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed, or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence. The Act applies to relevant competition offences as defined by the Competition Act 2002, the offences in question being those involving agreements between competing undertakings to prevent, restrict or distort competition.

3.17 The Act stipulates at section 4(5) that a superior officer making an application shall also have reasonable grounds for believing that the surveillance sought to be authorised is:

> "(a) the least intrusive means available, having regard to its objectives and other relevant considerations,
>
> (b) proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and
>
> (c) of a duration that is reasonably required to achieve its objectives."

3.18 The Act states that a judge issuing an authorisation may impose such conditions in respect of the surveillance as the judge considers appropriate.

3.19 Authorisation is required to be in writing and to specify:

> "(a) particulars of the surveillance device that is authorised to be used,
>
> (b) the person who, or the place or thing that, is to be the subject of the surveillance,
>
> (c) the name of the superior officer to whom it is issued,
>
> (d) the conditions (if any) subject to which the authorisation is issued, and
>
> (e) the date of expiry of the authorisation."

3.20 The authorisation shall expire on the date fixed by the judge that he or she considers reasonable and not later than three months from the date on which it is issued. There is provision to vary the authorisation or renew the authorisation, on the same or different conditions.

22. This refers to arrestable offences under:
"(a) section 186 of the Customs Consolidation Act 1876;
(b) section 1078 of the Taxes Consolidation Act 1997;
(c) section 102 of the Finance Act 1999;
(d) section 119 of the Finance Act 2001;
(e) section 79 (inserted by section 62 of the Finance Act 2005) of the Finance Act 2003;
(f) section 78 of the Finance Act 2005…"

3.21 There is also provision in section 7 for approval for surveillance in cases of urgency without prior judicial authorisation. The Act provides that a member of the Garda Síochána, an authorised officer of the Police Ombudsman or the Competition and Consumer Protection Commission, a member of the Defence Forces or an officer of the Revenue Commissioners may carry out surveillance without an authorisation if the surveillance has been approved by a superior officer.

3.22 A member or officer of one of the bodies in question may apply to a superior officer for the grant of an approval to carry out surveillance if he or she believes on reasonable grounds that requirements for an authorisation are fulfilled and that surveillance is justified, but that before an authorisation could be issued, it is likely:

> "(a) that a person would abscond for the purpose of avoiding justice, obstruct the course of justice or commit an arrestable offence, revenue offence or relevant competition offence, as the case may be,
>
> (b) information or evidence in relation to the commission of an arrestable offence, revenue offence or relevant competition offence, as the case may be, is likely to be destroyed, lost or otherwise become unavailable, or
>
> (c) the security of the State would be likely to be compromised."

3.23 The superior officer to whom an application is made shall approve the carrying out of such surveillance as he or she considers appropriate, if satisfied that there are reasonable grounds for believing that an authorisation would be issued, but that one or more of the conditions of urgency apply. The statute requires the superior officer approving the carrying out of surveillance to prepare a written record as soon as practicable and in any event, within eight hours. Surveillance under this approval procedure is confined to 72 hours. If the superior officer who approved surveillance believes on reasonable grounds that surveillance beyond the period of 72 hours is warranted, then he or she makes an application to a judge for an authorisation to continue the surveillance.

3.24 In the case of each of the bodies, there is provision for a report to be submitted to a high-ranking officer or official whenever the urgency provisions are invoked.

Tracking Devices

3.25 A quite different regime applies in the case of tracking devices. The movements of persons, vehicles or things may be monitored without prior judicial authorisation using a specified tracking device that has been approved by a superior officer.

3.26 A member or officer of one of the bodies may apply to a superior officer for the grant of an approval to use a tracking device if he or she believes that the requirements of the subsection dealing with applications for authorisation are fulfilled and that surveillance is justified, but that the use of a tracking device would be sufficient for obtaining the information or evidence in the circumstances concerned. The officer is also required to be of the opinion that the information or evidence sought could reasonably be obtained by the use of a tracking device for a specified period that is as short as is practicable to allow the information or evidence to be obtained.

3.27 As in the case of authorisations, there are requirements in relation to the recording of the grant of approval and for the making of a report to a high-ranking officer or official. The monitoring authorised is stated to be for a period of not more than four months (section 8(1)).

Retention of and Access to Material

3.28 Section 9 provides that applications for authorisation and supporting documentation shall be retained for a period of three years after authorisation ceases to be in force, or the day on which they are no longer required for any prosecution or appeal. There are similar provisions in respect of written records of approval, and reports and documents obtained as a result of surveillance or the deployment of a tracking device. The definition of "document" in statute includes any recording, including any data or information stored, maintained, or preserved electronically or otherwise than in legible form.

3.29 A further provision requires that documents shall be destroyed as soon as possible after they are no longer required to be retained. In section 9(5) it is stated that the Minister may authorise the retention of any of the documents referred to if he or she considers it necessary to do so,

> "having regard to—
>
> (a) the interests of the protection of the privacy and other rights of persons,
>
> (b) the security of the State,
>
> (c) the aims of preventing the commission of, and detecting, arrestable offences, and
>
> (d) the interests of justice."

3.30 Section 10 deals with storage and access to information and restrictions on disclosure of documentation. It was the section that was primarily in issue in *Hannaway*,[23] which was the only occasion on which this legislation has been considered by the Supreme Court. Section 10(1) stipulates that the Minister shall ensure that information and documents to which the Act applies are stored securely and that only persons that he or she authorises have access to them.

3.31 Subsection 2 states that the Minister may make regulations prescribing the persons or categories of persons who are to have access to information, the procedures and arrangements for secure storage, and the number of copies that may be made of documents, and the destruction of these copies.

3.32 Subsection 3 states that the Minister may make regulations respecting the disclosure of the existence of authorisations or approvals.

3.33 No such regulations have yet been made under either of these subsections. This will be discussed further at paragraph 3.78.

Complaints Procedure

3.34 The Act also provides for a complaints procedure. A person who believes that he or she might be the subject of an authorisation, or an approval may apply to the Complaints Referee. As mentioned previously, the Complaints Referee is an office first provided for by the Interception of Postal and Telecommunications Act 1993, but its remit has been extended to embrace surveillance as well as retention of data. It is an office that is usually held by a judge of the Circuit Court and is at present so held.

3.35 The Referee is required to investigate. If, after investigating the matter, the Referee concludes that there has been a relevant contravention, the Referee shall:

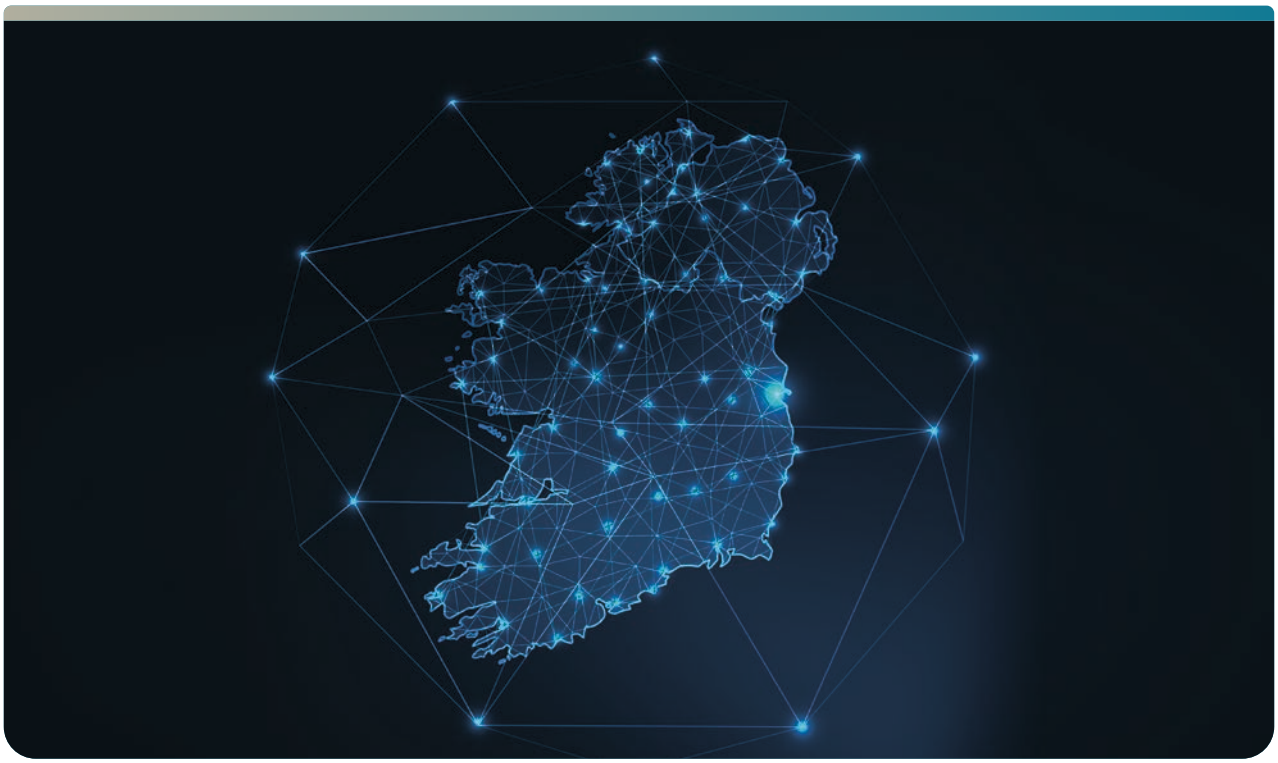
> "(a) notify the applicant, and any other person whose interests are materially affected by the relevant contravention, in writing of that conclusion, and
>
> (b) make a report of his or her findings to the Taoiseach."

3.36 There is also provision for the quashing of the authorisation or the reversal of the approval, the destruction of the records relating to the authorisation or approval and the destruction of any information or documents obtained.

3.37 The Referee also can make a recommendation for the payment of a sum, not exceeding €5,000, by way of compensation to the person who is the subject of the authorisation.

3.38 In the event of a conclusion that there has been a contravention, the Referee is also required to report the matter and any recommendation made by him or her to the Police Ombudsman, in the case of a contravention by An Garda Síochána; the Minister for Justice, Home Affairs and Migration, in the case of a contravention by the Police Ombudsman; the Minister for Enterprise, Tourism and Employment, in the case of a contravention by the Competition and Consumer Protection Commission; the Minister for Defence, in the case of a contravention by the Defence Forces; and the Minister for Finance, in the case of a contravention by the Revenue Commissioners.

23. Note 20.



3.39 On the other hand, if after investigating the matter, the Referee concludes that there has not been a relevant contravention, then the Act stipulates that the Referee shall give notice in writing to the applicant, stating only that there has been no such contravention. As mentioned earlier, this provision might be seen as an example of the principle of "neither confirming nor denying."

Admissibility of Evidence

3.40 One of the most significant sections of the Act is section 14, which provides that evidence obtained as a result of surveillance carried out under an authorisation or under an approval may be admitted as evidence in criminal proceedings. As we have seen, this was the aspect highlighted by the Minister in his second stage speech. There have been a number of high-profile criminal trials where surveillance evidence has featured, though such evidence is far from routine. While material gathered for surveillance will sometimes feature as evidence in criminal trials, this is to be contrasted with the situation in relation to lawful interception, which is used, in practice, exclusively as an intelligence-gathering tool.

Disclosure of Information

3.41 The statute restricts disclosure of information. Section 15 stipulates that unless authorised by the court, the existence or nonexistence of a number of matters shall not be disclosed by way of discovery or otherwise. The restriction applies to applications, authorisations and approvals, surveillance carried out under a judicial authorisation or under an approval, the use of a tracking device and the documentary or other information or evidence in relation to the decision to apply for an authorisation or an approval. The section provides that the court shall not authorise the disclosure, if it is satisfied that to do so is likely to present a risk to:

"(a) the security of the State,

(b) the ability of the State to protect persons from terrorist activity, terrorist-linked activity, organised crime and other serious crime,

(c) the maintenance of the integrity, effectiveness and security of the operations of the Garda Síochána, Police Ombudsman, Defence Forces, the Revenue Commissioners or the Competition and Consumer Protection Commission, or

(d) the ability of the State to protect witnesses, including their identities."

3.42 It then goes on to say at subsection 3 that the court may authorise the disclosure, subject to such conditions as it considers justified, if in all of the circumstances it is in the interests of justice to do so. As mentioned earlier, the approach taken in this regard may be contrasted with the more absolutist position of section 12 of the 1993 Act.

3.43 In the course of her judgment in *Hannaway*,[24] O'Malley J. at paragraph 117 commented that: "…there may be … cases where the defence suspect that surveillance was carried out and that evidence about such surveillance, or resulting therefrom, might be of assistance." At paragraph 129, she noted that such cases might include situations where the belief evidence of a chief superintendent could be undermined by recordings of an accused person's conversations with known members.

3.44 These comments provide support for the view that the more modern and nuanced approach to disclosure in the 2009 Act is to be preferred to the approach that was taken back in 1993 in relation to interception.

Review Visits

3.45 As already mentioned in this report, I have conducted three rounds of review visits, the first taking place post establishment day, with follow-up visits in September/October 2025 and January/February 2026.

An Garda Síochána

3.46 In the case of An Garda Síochána, during the period under review, the exercise of statutory surveillance powers was centralised within the Security and Intelligence section. Requests from gardaí at a district or divisional level are channelled through this section. It will frequently be the case that observational surveillance has already taken place in that a particular location or a particular individual has been monitored or observed. If the assessment of local gardaí is that more is required, an intelligence request may then be filed. The request will be interrogated, and in particular, the question of whether any less intrusive approach would serve the needs of the investigation will be explored. The fact that applications must be submitted to a centralised specialist unit has served as a very valuable internal quality control.

3.47 The Security and Intelligence section assesses what is needed and what resources are available. If the decision is to deploy a tracking device, that can proceed on the authority of a superintendent. If the deployment of an audio or audio-visual surveillance device is regarded as appropriate, that will necessitate an application to the District Court.

3.48 In general, An Garda Síochána resorts to statutory surveillance powers, whether involving tracking devices or surveillance devices, for a short period of time. Frequently, the perceived need for surveillance will relate to a particular garda operation targeting specific criminal activity. There may, for example, be grounds to believe that particular criminal activity, perhaps involving the movement of drugs or firearms, is to take place during a specified time period over coming days and this will determine the duration of surveillance.

3.49 On my first visit, I reviewed the files relevant to the period from establishment day to the date of that visit. The level of surveillance was not such that it could be regarded as extensive, still less excessive, nor did it suggest that surveillance was being resorted to regularly or as part of a fishing exercise. The files that I reviewed during my first visit and indeed on subsequent visits satisfied me that careful consideration was given to the question of whether surveillance was appropriate and proportionate, whether what was sought to be achieved required the use of a surveillance device, or whether, as was frequently the case, the deployment of a tracking device was deemed sufficient.

3.50 The level of surveillance carried out was broadly consistent with what had been reported on in the past by Designated Judges, if one excludes a particular time period when higher levels of surveillance were recorded. That period coincided with very high levels of organised criminal gang activity.

24. Note 20.

3.51 In addition to oversight visits, I visited the offices of the Assistant Commissioner with responsibility for Organised and Serious Crime at her invitation. This was in circumstances where a decision had been taken that this section will in the future have a role in exercising certain powers under the 2009 Act. We discussed the preparations that were then underway from both a technical and governance perspective. By year end, this section had not exercised statutory powers under the legislation. Its role in this area will be dealt with in the course of future reports.

The Defence Forces

3.52 Invocation of statutory surveillance powers and indeed, other statutory intrusive powers, by the Defence Forces is centralised within a particular unit, the Irish Military Intelligence Service (IMIS). I have previously referred to the fact that at an early stage, I was given a presentation on how various statutory powers had been invoked in the course of particular operations and the value of results obtained. Specifically, this was so in the case of surveillance.

3.53 The exercise of statutory powers in the Defence Forces tends to be for somewhat more extended periods. This is in contrast to the situation that prevails in An Garda Síochána, where certainly on the criminal investigation side, much of their surveillance activity is short-term, often linked to a specific event or a specific activity that is anticipated. I have commented elsewhere that this pattern of deployment for longer periods is quite understandable, given that threats to the security of the State tend to develop over a period and persist for a period.

3.54 Review of files over the three visits satisfied me that the powers were exercised with care and restraint. The paperwork was comprehensive and the case for engaging in surveillance and the necessity for doing so was set out in clear and cogent terms.

Fiosrú

3.55 Fiosrú did not rely on powers provided for by the 2009 Act during the period under review.

The Revenue Commissioners

3.56 In the course of engagement with the Revenue Commissioners, meetings focused very heavily on 2009 Act. Meetings were held with the principal officer who for a long time headed up the Revenue unit dealing with this area, with that officer's successor and with the Assistant Secretary in overall charge of the area.

3.57 In the case of Revenue, the number of files requiring review was modest. The vast majority of those involved internal decisions to make use of a tracking device, with only a very small number of applications to the District Court.

3.58 There is an internal review document, the *Tax and Duty Manual*, which sets out the procedures that are to be followed for applications under the 2009 Act. The decision to deploy a tracking device is considered internally. If the request for utilisation of a tracking device is approved by the superior officer/principal officer, the case then goes to the appropriate technical unit to give effect to the decision.

3.59 On two of the three review visits, in addition to reading the relevant files, I met members of the Revenue team who are tasked with carrying out surveillance. This was a very worthwhile exercise.

3.60 On every occasion, any questions that I had were carefully and comprehensively dealt with. Once again, I am satisfied that Revenue exercises its powers under the surveillance legislation in a restrained, responsible and entirely professional manner.

The Competition and Consumer Protection Commission

3.61 The Competition and Consumer Protection Commission (CCPC) has powers under both the Criminal Justice (Surveillance) Act 2009 and the Communications (Retention of Data) Act 2011, as amended. These powers are now provided for by the Competition (Amendment) Act 2022, which came into force on 27 September 2023. In the course of my first round of review visits, I did not visit the premises of the Competition and Consumer Protection Commission, because I had been informed that at that stage, the Commission had not yet exercised its recently acquired powers.

3.62 At an introductory meeting with the Commission following my designation, I met with those who will be leading Commission activity in this area, including a recently recruited staff member with a highly relevant background and considerable experience. During that initial discussion, I was struck by the fact that all senior personnel were keenly aware of the significance of the powers, and of how important it was that the powers would be exercised strictly in conformity with legislation and not invoked without full and careful consideration.

3.63 I visited the CCPC twice between September 2025 and February 2026 and was impressed with their preparations for use of the statutory surveillance powers, which had not been exercised by the end of the reporting period. I note that the necessary technical capability is now in place.

Incidence of Use of Statutory Powers

Statistics

3.64 During the period under review, An Garda Síochána made 9 applications to the District Court under section 4, all of which were granted under section 5, and 8 applications under section 6 for variation or renewals. In the previous year the comparable figures for the same 9-month period were 11 under section 5 and 6 under section 6. During both the period under review and the comparable period in 2024, An Garda Síochána did not avail of the section 7 urgency procedure. Tracking devices were deployed on 47 occasions, the comparable figure for the previous year being 41. There are no recorded instances in the period under review of applications to a senior officer being refused; a very small number of such refusals has been recorded in the past.

3.65 In the case of the Defence Forces during the period under review, there were 6 authorisations following applications under section 4. In 2024, there were no section 4 applications in the comparable period. There were no applications for approvals under section 8 for tracking devices in 2025, as was the case in the previous year. There were no applications for renewals and variations under section 6 and the section 7 urgency procedure was not invoked during this reporting period. Section 7 was used once during the same 9-month period in 2024.

3.66 The Revenue Commissioners made three section 4 applications during the reporting period, in comparison with one for the calendar year in 2024. There were no applications for variation or renewal of authorisations in the period under review, in comparison with one in the previous year. Section 7 was not invoked. There were 21 deployments of tracking devices during the period under review, compared to 22 in 2024.

Observations in Relation to the 2009 Act and Associated Recommendations

A Two-Tier Approach

3.67 As we have seen, the Act provides two distinct regimes, one for the deployment of audio and audio-visual devices and the other for the deployment of tracking devices. Surveillance devices other than tracking devices are only permitted to be deployed on foot of a warrant issued by a judge of the District Court, save in the case of urgency.

3.68 Although the Irish approach does not stand alone, the implicit assumption in the Act that surveillance by way of a tracking device is not overly intrusive, is open to challenge. By its nature, the use of a tracking device allows the precise location of the tracked vehicle or object to be determined over the period of time that the device is in use. This is likely to reveal significant details about the person(s) in control of the vehicle or object such as where they travel and when. In a series of cases in the retention of data field (discussed in more detail below), the Court of Justice of the European Union (CJEU) has held that particular categories of data, including location data in particular, may:

> "... reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health ... Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications... "[25]

3.69 Whilst acknowledging that surveillance and retention and access to data are separate fields, in my view, it is at least arguable that the logic of the CJEU's premise might apply by analogy with equal force to the information yielded by the use of tracking devices. Indeed, it could be argued that the CJEU's observations are even more pertinent in relation to the data available from tracking devices which are capable of being monitored in real time. This is in contrast to retained data, which are stored in largely anonymised form and the majority of which are never accessed.

3.70 It is, though, the case that in the United Kingdom, there is a two-tier approach to surveillance, which distinguishes between directed and intrusive surveillance, with greater restrictions in the latter case. The use of tracking devices falls within the category of the first tier, that of directed surveillance.

3.71 Some support for this approach may also be found in the decision of the European Court of Human Rights in *Uzun v Germany* (2011) 53 EHRR 24.[26] The applicant was a suspected member of an off shoot of the Red Army Faction. He had been convicted of attempted murder and causing explosions at the homes of members of parliament and the Peruvian consulate. Part of the evidence against him constituted surveillance data from a GPS tracking device and he argued that it was obtained in breach of his Article 8 ECHR private life rights. The ECtHR rejected this argument, finding that the stricter tests the Court had developed in the context of interception and surveillance of telecommunications were not directly applicable to tracking devices which "must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations..."[27]

25. Cases C-511/18, C-512/18 & C-520/18 *La Quadrature du Net v Premier Ministre* ECLI:EU:C:2020:791 at paragraph 117 [last accessed on 18 March 2026].
26. Available at https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-100293%22]} [last accessed on 18 March 2026].
27. Note 27 at paragraph 66 [last accessed on 18 March 2026].

3.72 In circumstances where an extension of statutory intrusive powers may be under evaluation, consideration might beneficially be given to the question of whether it remains appropriate to provide for the deployment of tracking devices without prior judicial authorisation. If the view was taken that requiring prior independent judicial authorisations on a blanket basis placed too great a burden on those exercising the powers and would prove impractical, 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 a requirement to then seek judicial ratification.

3.73 Another issue that merits consideration is whether there should be an express legislative requirement that senior officers dealing with urgent applications for surveillance and for applications for deployments of tracking devices should, in the light of the decision in *Damache v Director of Public Prosecutions* [2012] IESC 11, [2012] 2 IR 266,[28] be required to be independent of the investigation or operation. There will be further discussion of the implications of this case for legislation regulating intrusive powers in the retention of data section below.

Duration of Monitoring

3.74 Another issue in relation to tracking devices which merits further consideration is the duration of monitoring allowed by the legislation. Section 8(1) provides that:

> "notwithstanding sections 4 to 7, a member of the Garda Síochána, a designated officer of the Police Ombudsman, a member of the Defence Forces, an officer of the Revenue Commissioners or an authorised officer of the Competition and Consumer Protection Commission may, for a period of not more than 4 months or such shorter period as the Minister may prescribe by regulations, monitor the movements of persons, vehicles or things using a tracking device if that use has been approved by a superior officer in accordance with this section."

3.75 Two interpretations are arguably open. One is that in the absence of any specific provision for renewal of approval, further monitoring can take place following a subsequent application to a superior officer. Obviously, any such application would have to be on the basis of up-to-date information and intelligence, including information or intelligence acquired during the initial monitoring.

3.76 The alternative interpretation is that in the absence of specific provision for renewal of approvals for tracking devices, monitoring must cease after four months. Such an interpretation is a tenable one, particularly if account is taken of the fact that section 6 explicitly provides for renewal of other types of surveillance but not tracking devices. It is advisable that the matter be clarified and put beyond doubt by an appropriate amendment.

Retention of and Access to Material

3.77 As outlined, section 9 provides for a three-year retention period after an authorisation ceases to be in force or when no longer required for a prosecution or appeal. One can envisage situations where the requirement for destruction after three years could prove problematic. An example that comes to mind is if a prosecution was mounted a number of years after an incident was initially investigated, perhaps as a result of a cold case review. Another situation would be if there was a belated complaint to the Complaints Referee. These possible difficulties could be addressed by providing for a longer period of retention, but with very strict restrictions on access. While there would be something to be said for permanent retention with access only in exceptional circumstances and following independent authorisation, such a provision might run into difficulties in the light of some decisions of the European Court of Human Rights, such as *S and Marper v the United Kingdom* [2008] ECHR 1581, (2009) EHRR 50[29] and *Gaughran v United Kingdom* [2020] ECHR 144.[30] Consideration though should be given to providing for longer periods of retention of surveillance material, with appropriately strict restrictions on access.

3.78 As discussed, the absence of regulations under section 10 was at the heart of defence submissions in *Hannaway* before the Special Criminal Court and on appeal therefrom, which resulted in divergent approaches between the Supreme Court on the one hand, and the trial court and Court of Appeal on the other.

3.79 It goes without saying that this is an area of considerable sensitivity. If the rights of individuals are not to be infringed, it is vital that documentation be dealt with properly. While I have no reason to doubt the competence and professionalism of those charged with operating the legislation, I think it would be appropriate for the relevant Ministers to address these issues by way of regulation.

3.80 Professor Liz Heffernan, writing in the Irish Supreme Court Review, comments that the *Hannaway* case leaves the reader with the firm impression that the Oireachtas could, and should have, legislated for storage, access and disclosure in clearer, more explicit and comprehensive terms.[31] Whatever about the argument for more detailed primary legislation, there is clearly a strong argument for addressing this issue through secondary legislation.

28. Available at https://www2.courts.ie/acc/alfresco/cc9927d8-2a95-40e5-ba1f-2e996b7adb22/2012_IESC_11_1.pdf/pdf [last accessed on 18 March 2026].
29. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]} [last accessed on 18 March 2026].
30. Available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200817%22]} [last accessed on 18 March 2026].
31. Liz Heffernan, "Surveillance, Statutory Compliance and the Admissibility of Evidence: *DPP v Hannaway*" (2022) 4 *ISCR* 101.

SUMMARY OF RECOMMENDATIONS – 2009 ACT

- Provide for authorisation of tracking devices by superior officers on a short-term basis, with a requirement to seek judicial affirmation.
- Introduce legislative requirement for senior officers authorising urgent applications for surveillance or applications for tracking devices to be independent of the investigation or operation.
- Address the issue of the deployment of tracking devices after a period of four months' monitoring.
- Consider providing for longer periods of retention of surveillance material, with appropriately strict access restrictions.
- Make provision by Ministerial order for appropriate secure storage and restriction of access to surveillance material.

4

Communications (Retention of Data) Act 2011

Background to the Legislation

4.1 The Communications (Retention of Data) Act 2011 was the subject of very substantial amendment in 2022. It is the Act as amended that is the focus of attention.

4.2 The background to the 2011 Act in its present form is a complex one. To put it in context, it is appropriate to recall that in 2011, the Oireachtas enacted the Communications (Retention of Data) Act 2011 to give effect to Directive 2006/24/EC, usually referred to as the Data Retention Directive. In light of subsequent developments, it is worth reminding ourselves that prior to the enactment of the 2011 Act, Ireland was brought to the CJEU by the European Commission by reason of failure to transpose the 2006 Directive. In Case C-301/06 *Ireland v Parliament and Council* [2009] ECR I-593,[32] the State also challenged the legal basis for the Directive, contending that the European Union did not have competence in the area of criminal investigation and prosecution.

4.3 Against a background of the failed challenge and the infringement proceedings, the State moved to transpose the 2006 Directive into national law 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 Act provided for access to the retained data following a disclosure request made by a member of An Garda Síochána, not below chief superintendent rank or a member or officer of the Defence Forces or Revenue Commissioners of specified rank.

4.4 The provisions of the 2011 Act were subsequently challenged before the Irish courts in the case of *Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources* [2010] IEHC 221, [2010] 3 IR 251.[33] The High Court (McKechnie J.) made a preliminary reference to the CJEU which raised the validity of the 2006 Directive. In April 2014, the CJEU concluded[34] that the 2006 Directive was invalid, noting that it had caused a "wide-ranging" and "serious interference" with the rights to privacy and data protection enshrined in articles 7 and 8 respectively of the Charter of Fundamental Rights. The Court was of the view that the interference with Charter rights was disproportionate in light of the general character of the scheme of data retention provided for and the absence of any substantive and procedural conditions to prevent abuse.

4.5 In a series of decisions that followed, including Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson* EU:C:2016:970,[35] the Court addressed the ability of Member States to oblige communication service providers to retain traffic and location data in respect of all subscribers and registered users. In these cases, 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

32. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62006CJ0301 [last accessed on 18 March 2026].

33. Available at https://ww2.courts.ie/acc/alfresco/08a2f2b3-7bc4-473c-a9f1-0caf8fec4ece/2010_IEHC_221_1.pdf/pdf#view=fitH [last accessed on 18 March 2026].

34. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources and Proceedings brought by Kärntner Landesregierung and others* EU:C:2014:238. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293 [last accessed on 18 March 2026].

35. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203 [last accessed on 18 March 2026].

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.

4.6 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 very high-profile criminal proceedings. In January 2015, Graham Dwyer stood trial in the Central Criminal Court charged with murder. His victim had been reported missing in late August 2012. On 13 September 2013, human remains identified as those of the murder victim, Elaine O'Hara, were found by a person walking in the Killakee area of the Dublin mountains. Completely coincidentally, at the same time, a number of items were recovered from Vartry Reservoir, where water levels were unusually low. These items were linked to the missing person, whose remains had been found. Among these items were two mobile phones, complete with sim cards.

4.7 At trial, the prosecution case against Graham Dwyer depended in part on telephone evidence. There were a number of elements to this. In the first place, the prosecution sought to attribute three phones to the accused. One of these was referred to as a "work phone" and was registered to the accused's employer but was used by him. The prosecution sought to also attribute two other phones to him, of which he denied knowledge. The prosecution were particularly interested in a very large number of text messages that were passing between these two phones, which they argued should be attributed to the accused, and two phones that they were able to attribute to the deceased. The content of these messages was highly significant in enabling the identification of the sender of the messages to the phones linked to the deceased, and was also significant in providing information about the nature of the relationship between the accused and the deceased.

4.8 At trial, the accused sought to have the evidence of traffic and location data relating to the work phone – on which the prosecution placed reliance to assist in linking him to the two other phones – excluded on the ground that it had been retained and accessed in breach of EU law and was therefore, he argued, inadmissible. The contention placed reliance on the CJEU decision in *Digital Rights Ireland*. The arguments failed at trial. Following his conviction, Mr. Dwyer appealed to the Court of Appeal unsuccessfully[36] and further appealed to the Supreme Court, where he was again unsuccessful, with that Court delivering judgment on 31 July 2024.[37]

4.9 While the trial was taking place, Mr. Dwyer issued separate proceedings seeking declarations to the effect that the provisions of the Act which provided for the retention of and access to mobile phone data, including traffic and location data, were inconsistent with an EU Directive, Directive 2002/58/EC, sometimes referred to as the ePrivacy Directive. Following the annulment of the Data Retention Directive, the ePrivacy Directive was the principal Directive in the field. The High Court (O'Connor J.)[38] granted the declarations sought, declaring that sections 3(1), 6(1)(a) and 7 of the 2011 Act were inconsistent with Directive 2002/58 EC. The State defendants appealed and were permitted a leapfrog appeal to the Supreme Court. There it was decided that it was necessary to refer certain questions to the CJEU.[39] On 2 April 2022, the CJEU Grand Chamber gave judgment on the reference.[40]

36. *The People (DPP) v Graham Dwyer* [2023] IECA 70. Available at https://ww2.courts.ie/acc/alfresco/3d53966e-9888-4066-84a9-6f7766fe035b/2023_IECA_70.pdf/pdf#view=fitH [last accessed on 18 March 2026].

37. *The People (DPP) v Graham Dwyer* [2024] IESC 39. Available at https://ww2.courts.ie/acc/alfresco/e0339c95-8692-41b2-a5cc-0789284e4e38/2024_IESC_39_(Collins%20J)_Approved.pdf/pdf#view=fitH (Collins J.) and https://ww2.courts.ie/acc/alfresco/2b48bc0b-222a-4d48-bfb5-d4490a17ad63/2024_IESC_39_(Hogan%20J).pdf/pdf#view=fitH (Hogan J.) [last accessed on 18 March 2026].

38. *Graham Dwyer v Commissioner of An Garda Síochána* [2018] IEHC 685, [2019] 1 ILRM 461. Available at https://ww2.courts.ie/acc/alfresco/37f5f57c-0173-4e22-8cd8-d608d16fbe4f/2018_IEHC_685_1.pdf/pdf#view=fitH [last accessed on 18 March 2026].

39. *Graham Dwyer v Commissioner of An Garda Síochána* [2020] IESC 4, [2020] 1 ILRM 389. Available at https://ww2.courts.ie/acc/alfresco/4a0df0ae-b64d-4f3a-92d4-bf178dbbb43f/2020_IESC_4_Clarke%20CJ.pdf/pdf#view=fitH [last accessed on 18 March 2026].

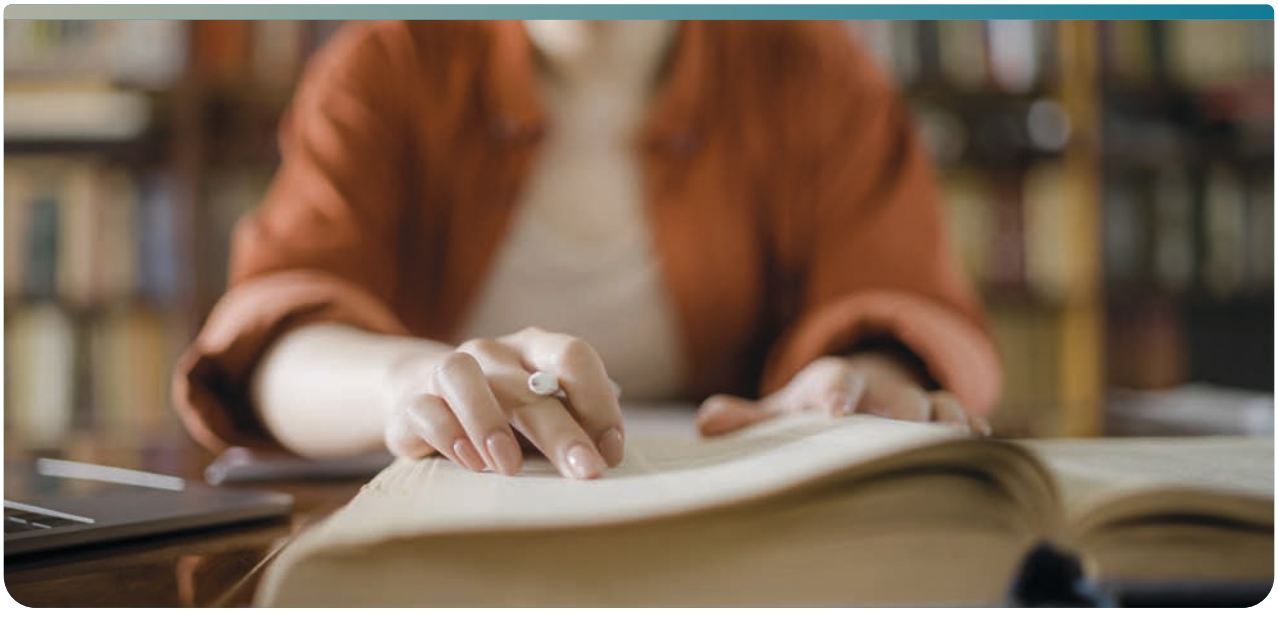
40. Case C-140/20 *GD v Commissioner of An Garda Síochána* EU:C:2022:258. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0140 [last accessed 18 March 2026].

4.10 The operative part of the judgment (the *dispositif*) is in these terms:

> "Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data."[41]

4.11 However, the Court also found that:

> "Article 15(1), read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for:
>
> - the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
> - the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
> - the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
> - recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,
>
> provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse."[42]



41. Note 40, paragraph 129(1).
42. Note 41.

4.12 The CJEU went on to hold that the Irish courts were precluded from limiting the temporal effects of the declaration of invalidity of the Data Retention Directive and its knock-on effect on the 2011 Act which implemented it. This meant that the "general and indiscriminate retention of traffic and location data" allowed by the Act was unlawful under EU law by virtue of Article 15(1) of Directive 2002/58, read in the light of the Charter of Fundamental Rights. However, the Court confirmed that the admissibility of evidence obtained by such retention is a matter for the Member State, subject to compliance with the EU law principles of equivalence and effectiveness.

4.13 Following the CJEU judgment, the Supreme Court proceeded to dismiss the appeal that had been before it and affirmed the order made by O'Connor J.

Legislative Response

4.14 The legislative response to these developments was the enactment of the Communications (Retention of Data) (Amendment) Act 2022 (the "2022 Act"). The general approach taken by the 2022 Act 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 communications data for reasons of national security and for criminal law enforcement purposes.

4.15 The Act categorises data into "user data", "Schedule 2 data" and "internet source data".

4.16 User data includes:

- user ID,
- name and address of subscriber,
- mobile or fixed telephone number,
- International Mobile Subscriber Identity (IMSI),
- International Mobile Equipment Identity (IMEI) and the like.

4.17 Schedule 2 data, commonly referred to as traffic and location data, is data necessary to trace and identify:

- the source of the communication,
- the destination of a communication,
- the time and date of the start and end of a 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 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 is terminated.

4.18 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:

(a) the Internet Protocol (IP) address, whether dynamic or static, allocated by the service provider to the source of a communication;

(b) 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."

4.19 The legislation provides for different regimes for retention and access in each case. In the case of access, there is essentially a tiered regime, with the provisions applicable to Internet Source Data and Schedule 2 data being more demanding. 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.

4.20 Alongside the distinction based on the nature and categorisation of the data, there is a second differentiation based on the purpose for which access is sought, with the distinction drawn depending on whether what is in issue is State security or whether what is in issue relates to criminal investigation or other permitted purposes.

4.21 The distinction between State security and other purposes for which access might be sought can be traced directly to decisions of the CJEU. How the Court dealt with that issue in the course of its judgment in the *GD* case merits quotation at some length, because it has had such an influence on our current legislation in this area.

4.22 In paragraph 58 and subsequent paragraphs, the Court observed as follows:

> "58. It is for that reason that the court held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a Court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists…
>
> "59. As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general …
>
> "60. At the hearing, the European Commission submitted that particularly serious crime could be treated in the same way as a threat to national security.
>
> "61. However, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities…
>
> "62. It should also be observed that, unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed…

"63. Thus, criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. As the Advocate General observed in points 49 to 50 of his Opinion, to treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former."

4.23 In a situation where the effective legislation in this area is recent, having been provided for by the Communications (Retention of Data) (Amendment) Act 2022, and in circumstances where the principal Act required to be reported on, the Act of 2011, has been the subject of very radical amendment, it seems appropriate to offer an overview of the current legislation. In seeking to do this, I acknowledge that I have drawn heavily from the revised and updated version of the 2011 Act, prepared by the Law Reform Commission.[43]

Statutory Provisions

Data Retention

4.24 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 Minister may prescribe a period that is less than one year but not one that exceeds two years. The Minister has not made specific regulations under this section, however the issue is addressed by the Communications (Retention of Data) (Data Security) Regulation 2023 (S.I. 352/2023).[44]

4.25 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.

4.26 Section 3A 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 under this section. Subsection 2 provides that before making an application, the Minister shall assess the threat to the security of the State, and in doing so, shall have regard to the necessity and proportionality of the retention of Schedule 2 data, taking into account the impact of such retention on the fundamental rights of individuals.

4.27 Subsection 3 stipulates that the application to Court by the Minister will be made *ex parte*, upon information on oath specifying the grounds on which the order is sought; this will include the assessment of the threat to the security of the State. The application must also specify the period of time for which the Minister believes that the retention of Schedule 2 data is required for the purposes of safeguarding the security of the State. It is also provided that the application would be heard otherwise than in public.

4.28 Subsection 4 states that a relevant judge, when dealing with an application, may make an order requiring service providers to retain Schedule 2 data, only if satisfied that the making of such an order is necessary for and proportionate to the purposes for which the application was made. An order made under the subsection requires all service providers to retain Schedule 2 data, or such data as specified in the order, for a period of 12 months from the date on which the data was first processed.

4.29 Two judges of the High Court have been designated by the President of that Court to perform the functions of a relevant judge. One of the judges designated as a relevant judge, Owens J., made such an order on 26 June 2023 and similar orders on 21 June 2024 and 20 June 2025.

4.30 Service providers are required by section 3B to retain internet source data for a period of one year or such period as maybe prescribed.

43. Available at https://revisedacts.lawreform.ie/eli/2011/act/3/front/revised/en/html [last accessed on 18 March 2026].

44. Available at https://www.irishstatutebook.ie/eli/2023/si/352/made/en/print [last accessed on 18 March 2026].

Data Security

4.31 At section 4 of the legislation, the issue of data security is addressed. Service providers are required to take specified security measures in relation to retained data. Data are required to be retained for one year and shall be destroyed thereafter by the service provider, except those that have been accessed and preserved. The Communications (Retention of Data) (Data Security) Regulations 2023 (S.I. 352/2023) specifies 13 months from the date on which the data were first processed by the service provider and one month from the date on which a preservation order ceases to have effect, as the dates by which the data must be destroyed.

Requirement to Disclose User Data

4.32 Section 6 deals with requirements to disclose user data. It provides that:

> "(1) A member of the Garda Síochána not below the rank of superintendent may require a service provider to disclose to that member user data in the possession or control of the service provider—
>
> (a) where the member believes that the data relate to a person whom the member suspects, on reasonable grounds of—
>
> (i) having committed an offence, or
>
> (ii) presenting an actual or potential threat to the security of the State,
>
> or
>
> (b) where the member has reasonable grounds for believing that the data are otherwise required for the purpose of—
>
> (i) preventing, detecting, investigating or prosecuting offences,
>
> (ii) safeguarding the security of the State,
>
> (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) determining the whereabouts of a missing person.

"(2) A member of the Permanent Defence Force not below the rank of lieutenant colonel may require a service provider to disclose to that member user data in the possession or control of the service provider—

(a) where the member 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

(b) where the member has reasonable grounds for believing that the data are otherwise required for the purpose of safeguarding the security of the State.

"(3) An officer of the Revenue Commissioners not below the rank of principal officer may require a service provider to disclose to that officer user data in the possession or control of the service provider—

(a) where the officer believes that the data relate to a person whom the officer suspects, on reasonable grounds, of having committed a revenue offence, or

(b) where the officer has reasonable grounds for believing that the data are otherwise required for the purpose of preventing, detecting, investigating or prosecuting a revenue offence."

"Revenue offence" is defined by reference to a number of statutory provisions in similar terms to that found in the Criminal Justice (Surveillance) Act 2009.

"(4) An officer of the Competition and Consumer Protection Commission not below the rank of principal officer may require a service provider to disclose to that officer user data in the possession or control of the service provider—

(a) where the officer believes that the data relate to a person whom the officer suspects, on reasonable grounds, of having committed a competition offence, or

(b) where the officer has reasonable grounds for believing that the data are otherwise required for the purpose of preventing, detecting, investigating or prosecuting a competition offence."

4.33 There is a statutory definition of a competition offence which accords with that contained in the Criminal Justice (Surveillance) Act 2009.

4.34 It may be noted that the member of An Garda Síochána may require disclosure where the member believes that the data relates to a person suspected on reasonable grounds of having committed "an offence." This is to be contrasted with other provisions relating to the exercise of intrusive powers where one finds reference to "serious offences" or "arrestable offences." On this occasion, the reference is to "offence", without qualification.

4.35 The Act provides that the member or officer concerned makes their requirement for disclosure by notice in writing, but there is a provision in circumstance of exceptional urgency for the requirement to be other than in writing, in which case notice in writing within two days is required.

Authorisation Required for Disclosure of Schedule 2 Data

4.36 Provision is made for a member of An Garda Síochána, not below the rank of inspector, or a member of the Permanent Defence Forces not below the rank of commandant to apply to an authorising judge, a judge of the District Court designated by the President of the District Court, where the member is of belief that the Schedule 2 data in question:

"(a) 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

(b) are otherwise required to be preserved for the purpose of safeguarding the security of the State."

4.37 The issuing judge may issue the authorisation only if satisfied the relevant criterion is applicable and that the issuing of the authorisation is necessary for and proportionate to the purposes for which the application is made.

4.38 In cases of urgency, there is provision for an application to a superior officer. What is required is that the member making the application to the superior officer is of the reasonable belief that the data relate to a person whom the member suspects, upon reasonable grounds of presenting an actual or potential threat to the security of the State or otherwise required for the purpose of safeguarding the security of the State. The member must also be of the belief that before the Schedule 2 data could be obtained pursuant to an authorisation from a judge, that:

> "(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or
>
> (ii) the security of the State would be compromised."

4.39 There is an obligation on the superior officers to prepare a record in writing and to submit that report to a person of specified seniority in the organisation. There is also a requirement to apply to an authorising judge for affirmation of the authorisation. It is specified that an application for an authorisation shall not be made to a superior officer who has had any involvement in the investigation, detection or prevention of a threat or apprehended threat to the security of the State that occasioned the making of the application and that such a superior officer shall not consider an application or issue an authorisation. This is of some interest in the context of other legislation regulating the use of intrusive powers such as the 2009 Act. This (and similar provisions, which are to be found at a number of places in the Act) is prompted by a desire to respond to the decision in *Damache v Director of Public Prosecutions*. The approach taken mirrors the architecture of the Criminal Justice (Search Warrants) Act 2012, which permits garda superintendents and officers of higher rank to issue warrants in circumstances of urgency, but only if independent of the investigation of the offence.

Accessing Internet Source Data

4.40 A member of An Garda Síochána not below the rank of inspector may apply to an authorising judge for an authorisation under this section where the member is of the belief that the internet source data in respect of which the application is made:

> "(a) relate to a person whom the member suspects, on reasonable grounds of—
>
> (i) having committed a serious offence, or
>
> (ii) presenting an actual or potential threat to the security of the State,
>
> or
>
> (b) are otherwise required to be preserved for the purpose of—
>
> (i) preventing, detecting, investigating or prosecuting a serious offence,
>
> (ii) safeguarding the security of the State,
>
> (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) determining the whereabouts of a missing person."

4.41 It may be noted that in contrast to the section relating to user data, the belief or reasonable suspicion on the part of the member of An Garda Síochána has to be that the person is suspected of having committed a serious offence.

4.42 Likewise, in the case of the Defence Forces, a member not below the rank of commandant may apply to an authorising judge for an authorisation under this section where the member is of the belief that the internet source data in respect of which the application is made:

> "(a) relate to a person whom the member suspects, upon reasonable grounds, of presenting an actual or potential threat to the security of the State, or
>
> (b) are otherwise required for the purpose of safeguarding the security of the State."

4.43 Officers of the Revenue Commissioners and of the Competition and Consumer Protection Commission, not below the rank of assistant principal may also apply. The Revenue officer may do so when of the belief that the internet source data in respect of which the application is made:

"(a) relate to a person whom the officer suspects, on reasonable grounds, of having committed a revenue offence, or

(b) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a revenue offence."

4.44 The Competition and Consumer Protection Commission officer must similarly be of the belief that the internet source data in respect of which the application is made:

"(a) relate to a person whom the officer suspects, on reasonable grounds, of having committed a competition offence, or

(b) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a competition offence."

4.45 Section 6C(6) specifies that the authorising judge may issue an authorisation only if satisfied that the particular criterion is made out and that the issuing of the authorisation is necessary for and proportionate to the purpose for which the application was made.

4.46 There is provision at section 6D for authorisations to require disclosure of internet source data in cases of urgency. This involves applications by officers or members of specified rank to a senior officer. What is required in such an application is that the applicant believes on reasonable grounds that the basis for applying to an authorising judge is present, and believes that before the internet source data could be obtained pursuant to a judicial authorisation, the data would be wholly or partly destroyed or otherwise rendered unavailable and that the security of the State would be compromised and the achievement of an objective of preventing, detecting, investigating or prosecuting a serious offence, safeguarding the security of the State, protecting the life or personal safety of a person or determining the whereabouts of a missing person, or preventing, detecting, investigation or prosecution of a revenue offence or competition offence would be impeded.

4.47 The Act contains detailed provisions imposing obligations on the superior officer to whom the application is made to create a record of the authorisation and to submit a report, in the case of An Garda Síochána, to a member of An Garda Síochána not below the rank of chief superintendent; in the case of the Defence Forces, to a member not below the rank of colonel; to an officer not below the rank of assistant secretary general in the case of the Revenue Commissioners; and a person of the rank of member of the Commission in the case of the Competition and Consumer Protection Commission.

4.48 There is also provision requiring the superior officer as soon as possible and, in any event, not later than 72 hours, to apply to an authorising judge for affirmation.

4.49 As in the case of Schedule 2 data urgency provisions, it is stated that the application for authorisation is not to be made to a superior officer who has had prior involvement in the matter that gave rise to the application.

Cell Site Data

4.50 Section 6E of the Act makes specific provision for the requirement to disclose cell site location data in situations of urgency. This provides that a member of An Garda Síochána not below the rank of inspector may apply to a superior officer for an authorisation under this section, where the member believes on reasonable grounds that the cell site location data in respect of which the application was made are required for the purpose of:

"... (a) 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

(b) determining the whereabouts of a missing person.

(2) A superior officer to whom an application under subsection (1) is made shall issue an authorisation under this section only if satisfied that—

(a) paragraph (a) or (b) of the subsection applies in respect of the cell site location data concerned,

(b) the issuing of the authorisation is necessary for, and proportionate to, the purposes for which the application is made, taking into account the impact of the disclosure of the cell site location data concerned pursuant to the authorisation on the fundamental rights of individuals, and

(c) the circumstances of urgency giving rise to the application would render it impracticable to seek to achieve the objective specified in paragraph (a) or (b) of subsection (1), as the case may be, under any other provision of this Act."

4.51 Unusually, notwithstanding the general statutory definition of superior officer meaning in the case of An Garda Síochána, a member not below the rank of superintendent, for the purpose of this section, the definition means a member not below the rank of inspector. This seems to give rise to the possibility of an inspector making an application to another inspector. However, my understanding is that the arrangements in place within An Garda Síochána ensure that in practice, applications are always made by an inspector to a superintendent.

4.52 Section 6E contains the now familiar stipulation that an application for an authorisation shall not be made to a superior officer who has had any involvement in an action taken by An Garda Síochána in response to the circumstances that occasioned the making of the application, and that such an officer shall not consider an application or issue an authorisation.

4.53 The application can only be made when the member of An Garda Síochána believes that the cell site location data is required for the purpose of protecting the life or personal safety of a person, where the member believes there is a serious risk to the life or personal safety of the person, or for the purpose of determining the whereabouts of a missing person.

4.54 Given the very restricted circumstances in which urgent applications for cell site location data can occur, I am not at all convinced that the provision excluding a superior officer with a prior involvement in the investigation is necessary or appropriate. Where the matter in issue is protecting the life or personal safety of a person, or locating the whereabouts of a missing person, it would not be at all unusual for this to arise in circumstances of urgency, and indeed, extreme urgency. The section recognises that urgency is likely to be a feature of such cases by defining "superior officer" for this purpose as a member not below inspector rank.

4.55 I believe that the exclusion of superior officers with prior involvement achieves little but adds an unnecessary complication. I therefore recommend that consideration should be given to providing for exceptions to this requirement.

Preservation and Production Orders

4.56 A significant feature of the legislation is that it provides for the creation of two new types of legal orders, preservation and production orders. In the case of these two new orders, as we have seen elsewhere, the norm is an application to an authorising judge, with provisions made for situations of urgency through temporary preservation and temporary production orders.

4.57 The preservation order has been described as a "quick freeze".[45] Of note, a preservation order is not a necessary precondition for the making of a production order.

4.58 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 applying 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 is 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 a 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).

4.59 On the other hand, if the data are sought for other purposes, then the data that can be accessed include data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order other than an order under section 3A or a preservation order under subsection (4). 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 sought for reasons other than State security, or to put it slightly differently, data that exists by reason of the existence of a section 3A order can be the subject of a preservation or production order obtained on national security grounds pursuant to section 6A, but will not be subject to an order applied for on any other ground.

Absence of Express Reference to Fiosrú

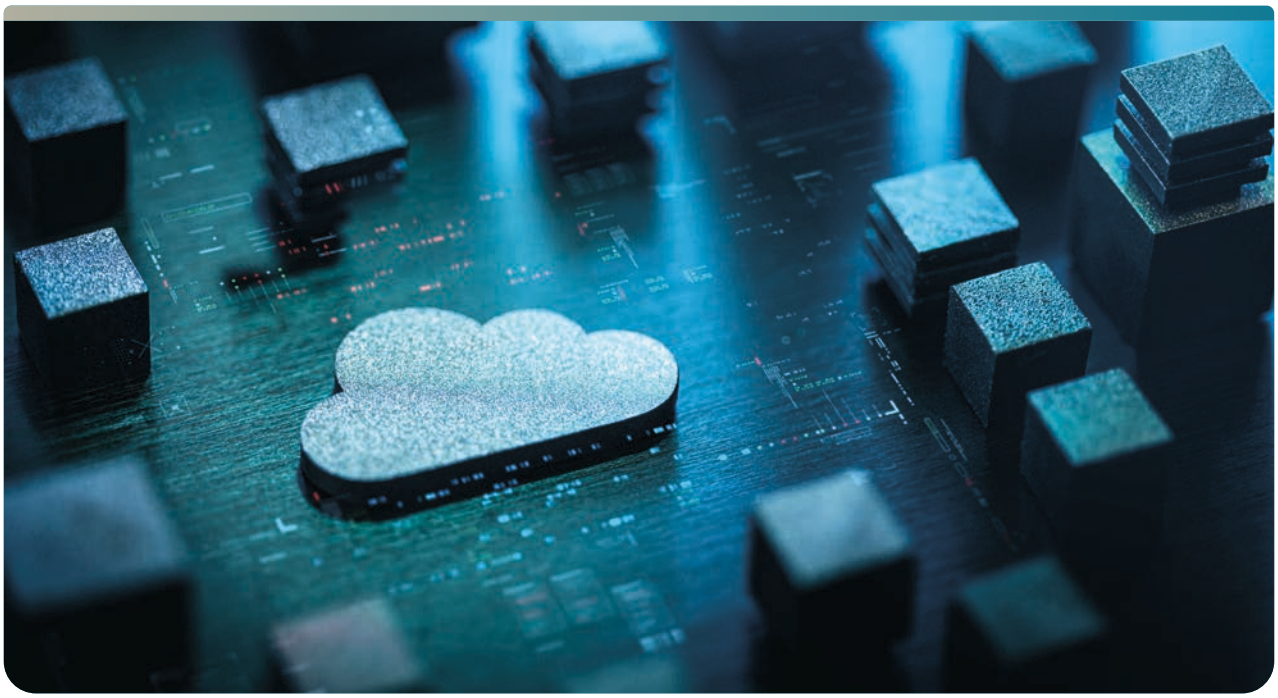
4.60 The Act makes no specific reference to Fiosrú or to the Police Ombudsman. At a number of levels, that may be seen as surprising and indeed unsatisfactory. It is the case that Fiosrú and its predecessor have a long history of activity under the 2011 Act. In those circumstances, one would expect, given the intrusive nature of the powers provided for in this area, that there would be absolute clarity as to what bodies are exercising powers. That general expectation is heightened when one has regard to the fact that the legislation regulating intrusive powers in other areas (lawful interception and surveillance) makes specific reference to a role for the Police Ombudsman.

4.61 The absence of any express reference to the Police Ombudsman or Fiosrú is particularly hard to understand, given that the issue was directly addressed in the report of the former Chief Justice, the late John Murray in April 2017. At paragraph 372, he commented:

> "…there is an evident need for greater clarity and certainty in the matter of GSOC's entitlement to make disclosure requests pursuant to section 6 of the 2011 Act. As already indicated, given the highly intrusive nature of a system of data retention and disclosure, and the concomitant threats it poses to the fundamental rights of those affected by its operation, it is essential that all avenues of access to private data should be expressly provided for within the framework of the governing enactment in the area. In short, the governing enactment should comply with the legality or clear statement principle, while legislative scatter in the matter of access should be avoided at all costs. Plainly the provisions of the principal enactment should specify the bodies entitled to issue disclosure requests; and the list of bodies thus specified should be exhaustive."[46]

45. See statement by the then Minister for Justice: "Minister McEntee commences Act to facilitate retention of data to protect national security and tackle serious crime", 6 June 2023 [last accessed on 18 March 2026].

46. For a similar view, see Shane Kilcommins and Eimear Spain, "GSOC, the Legislative Process and the Privacy Rights of Citizens" (2017) 27 (4) *Irish Criminal Law Journal* 145. Draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600698 [last accessed on 18 March 2026].



4.62 The *Report on Pre-Legislative Scrutiny of the Communications (Retention of Data) Bill 2017* by the Joint Committee on Justice and Equality referred to the fact that head 5 of the Bill, which was then under consideration, made specific reference to GSOC. On page 5 of the report, the Committee referred to the criticism of the lack of coherence and clarity in data retention law at that time, which it was pointed out was described in the Murray Report as "legislative scatter". They noted, with apparent satisfaction, that a number of heads of the Bill under consideration addressed the criticisms and expressly covered GSOC and how it may request and use retained data.

4.63 The Murray Report explained that GSOC placed reliance on section 98(1) of the Garda Síochána Act 2005, which provides that:

> "If directed by the Ombudsman Commission under section 91(2)(b), 92(c), 94(8)(a) or 94(11)(b) to investigate a complaint under this section, a designated officer has, in relation to the member of the Garda Síochána under investigation, for the purposes of the investigation all the powers, immunities and privileges conferred and all the duties imposed on any member of the Garda Síochána by or under any enactment or the common law, including those relating to the following matters:
>
> (a) the entry and search of any place (other than a Garda Síochána station) pursuant to a warrant issued in accordance with law and the seizure of things authorised by the warrant;
>
> (b) the arrest, with or without a warrant, of a person;
>
> (c) the bringing of a charge against a person;
>
> (d) the issue of a summons to a person;
>
> (e) the search of a person and the taking of his or her photograph, fingerprints and palmprints;
>
> (f) the detention and questioning of a person;
>
> (g) the taking of bodily samples or other things from a person for the purpose of forensic testing."

4.64 Having quoted the subsection, the former Chief Justice points out that the subsection goes on to specify certain matters, none of which specifically refer to a power to access retained data. The comparable current statutory provision is section 209 of the Policing, Security and Community Safety Act 2024. Given its importance, and at the risk of repetition, it is worth quoting that section in full:

"(1) Where a designated officer is appointed under *section 208(1)* to undertake an investigation, any designated officer shall, for the purposes of undertaking, or assisting in, the investigation concerned and any matters ancillary or consequential to such an investigation, have all the powers, immunities and privileges conferred, and all the duties imposed, on any member of An Garda Síochána by or under any enactment or the common law, including those relating to the following matters:

(a) the entry and search of any place (other than a Garda Síochána premises) pursuant to a warrant issued in accordance with law and the seizure of things authorised by the warrant;

(b) the arrest, with or without a warrant, of a person;

(c) the bringing of a charge against a person;

(d) the issue of a summons to a person;

(e) the search of a person and the taking of his or her photograph, fingerprints and palmprints;

(f) the detention and questioning of a person;

(g) the taking of bodily samples or other things from a person for the purpose of forensic testing.

(2) For the purposes of *subsection (1)*, an enactment conferring a power, immunity or privilege or imposing a duty on a member of An Garda Síochána in relation to any of the matters specified in that subsection applies with the following modifications and any other necessary modifications:

(a) subject to *paragraph (c)*, a reference in the enactment to a member of An Garda Síochána shall be construed as a reference to a designated officer;

(b) a reference in section 4 of the Criminal Justice Act 1984 or in the Regulations of 1987 to a member in charge of a Garda Síochána station shall be construed as a reference to a designated officer;

(c) a reference in the enactment to a member of An Garda Síochána not below the rank of inspector shall be construed as a reference to a senior designated officer.

(3) Any person who delays, obstructs or interferes with a designated officer in the exercise of the powers conferred, or the carrying out of the duties imposed, under *subsection (1)* is guilty of an offence and is liable, on summary conviction, to a class B fine or imprisonment for a term not exceeding 12 months, or both.

(4) In this section—

"enactment" means a statute or statutory instrument, whether passed or made before or after the passing of this Act or any portion of such a statute or statutory instrument, but does not include any provision of the Offences against the State Acts 1939 to 1998."

4.65 Murray C.J.'s observations might have been thought to be particularly significant given that the review he was conducting was prompted by public concern in the wake of GSOC relying on section 6 of the 2011 Act to access phone records of journalists.

4.66 The former Chief Justice would appear to have had some doubts about the correctness of the interpretation of section 98(1) of the Garda Síochána Act 2005, commenting at paragraph 371 of his report that "GSOC's interpretation to the contrary notwithstanding, it is not self-evident that the terms of section 98(2)(c) necessarily comprehend the powers reserved to an officer of the Garda Síochána not below the rank of superintendent which is the designation in section 6 of the 2011 Act."

4.67 I would echo the language about the situation not being self-evident, but I am prepared to accept that the interpretation by GSOC and its successor is probably correct. I am, though, of the opinion that the interpretation gives rise to some anomalies.

4.68 By statute, a senior designated officer holds a rank equivalent of "not below inspector." The architecture of the 2011 legislation envisages occasions when a person of a particular rank makes an application to a person of higher rank. By way of one example of the many that are available, section 6B of 2011 Act deals with a situation where a member of An Garda Síochána not below the rank of inspector may apply to a superior officer for an authorisation to require disclosure of schedule 2 data in cases of urgency.

4.69 If ranks within Fiosrú are to be equated with Garda Síochána ranks, it could see a senior designated officer making an application to another, similarly ranked senior designated officer. My understanding is that there are arrangements in place internally within Fiosrú that see a senior designated officer making an application to a person who is, in fact, more senior in rank terms to the person applying. The apparent anomaly is perhaps not as significant in practice as might appear for that reason. Also, as mentioned, the anomaly is not unique in that the 2011 Act appears to contemplate a situation where an inspector of the Garda Síochána might apply to another inspector to approve the disclosure of cell site location data in cases of urgency (section 6E).

4.70 A further anomaly arises in relation to the statutory provisions for creating a statistical record of data retention and access. Section 9 deals with the preparation of reports by the Garda Commissioner, the Chief of Staff, the Revenue Commissioners and the Competition and Consumer Protection Commission. Reports prepared and submitted are then required, having been reviewed by the relevant Minister, to be forwarded to the Minister for Justice, Home Affairs and Migration, who is then required to prepare a consolidated report and submit it to the European Commission. There is no reference in this section to Fiosrú, which means that any report prepared strictly in accordance with this statutory provision would not be fully comprehensive. This is, in truth, of limited significance in practical terms, as the European Commission no longer plays the role it had been given by the Data Retention Directive before it was struck down.

4.71 If the view is taken, as I think is in fact the case, that the Police Ombudsman should have the same powers available to her in this area as those that are available to An Garda Síochána, that should be specifically and directly provided for by statute. I recommend that a suitable vehicle be found for the early enactment of legislation in that regard.

Review Visits

4.72 In the course of each round of review visits, I engaged with all those exercising intrusive powers under the Act.

An Garda Síochána

4.73 In the case of An Garda Síochána, during the first round, I actually had two engagements in relation to data retention, because I sought further clarification on particular procedural and technical points. The additional meeting with the officers directly involved was arranged very quickly and all my queries were answered in a comprehensive way.

4.74 During a subsequent visit, my attention was drawn to two occasions on which errors had been identified. One error was made in respect of one digit in an 11-digit IP address, which was the subject of a request for internet source data. The error was noticed by the service provider, which drew the attention of An Garda Síochána to the matter.

4.75 The second error was similar in nature. An investigator sought user data for a particular mobile phone and there was an error in respect of one digit, where a number 1 and number 7 were confused. In this case, the investigator identified the error and no action was taken on the results initially returned.

4.76 In these cases, the errors did not give rise to any real consequences. However, it is by no means inconceivable that in a different situation, an error of that sort might have significant consequences. For that reason, I have requested all authorised bodies to bring any error to my attention without delay as soon as identified. This is a practice that might with benefit be put on a statutory basis in the future.

The Defence Forces

4.77 As indicated, IMIS gave a detailed account of how this and other intrusive powers had been used in particular cases and what outcomes had been achieved. This presentation, and my review of relevant individual files, satisfied me that the legislation is used with restraint and in a responsible manner. The legislation is clearly of value to the Defence Forces as they go about their work.

The Revenue Commissioners

4.78 During the period under review, Revenue did not exercise any of their powers under the Act.

Fiosrú

4.79 At my meetings with Fiosrú, I was struck by the seriousness with which senior people there were taking the exercise of statutory powers. All or part of meetings were attended by the Ombudsman or Deputy Ombudsman, along with the senior officials having direct responsibility in the area.

4.80 Any proposal to exercise statutory powers is reviewed at a number of different levels in the organisation. It is considered at investigator level, senior investigator level, by the head of the Digital Investigations Unit and at Deputy Director level. It was explained to me that even in cases where it might be possible under the legislation to proceed without the necessity for an application to court, the view is taken within the organisation that a court application is preferable.

The Competition and Consumer Protection Commission

4.81 As already indicated, by year end, the CCPC had not exercised any statutory powers. Our meetings were forward-looking, focusing on discussing the sort of occasions on which it was envisaged there might be resort to the statutory powers in the future and the procedures that would be followed in those situations.

Incidence of Use of Statutory Powers

Statistics

4.82 Between 2 April and 31 December 2025, all of the agencies vested with statutory powers with the exception of the Revenue Commissioners and the Consumer and Competition Protection Commission exercised those powers.

4.83 In the case of An Garda Síochána, during the period under review, there were 1292 requests for user data, 403 requests for internet source data and 32 requests for cell site location data in cases of urgency. There were 9 preservation orders sought under section 7A and 116 production orders under section 7C. For the same period in 2024, there were 944 requests for user data, 659 requests for internet source data and 58 requests for cell site location data in cases of urgency. There was 1 preservation order sought under section 7A and 73 production orders under section 7C.

4.84 The Defence Forces made 83 requests for user data during the period under review. For the same period in 2024, there were 30 requests.

4.85 Fiosrú made 27 user data requests and two applications for production orders.

4.86 In other contexts, I have made the point that statistics in this area have to be treated with caution because there might be a number of applications in relation to a single individual, either because the individual is believed to use more than one phone or to move between networks, or there is uncertainty about which network he or she is on.

Observations in Relation to the 2011 Act

Data Retention for Criminal Investigation

4.87 The striking feature of the legislation is the absence of a general obligation to retain data for the purpose of access in the course of investigations of serious crime. How that has come about is described above, and the reality is that there may be little that the government or the Oireachtas can do about it, other than advocating for change at EU level, but the situation is in my view less than satisfactory. In the course of his judgment in *Graham Dwyer*, dissenting from his colleagues when they decided to make a reference to the CJEU, Charleton J. pointed to the importance of metadata evidence in trials arising from the murder of Veronica Guerin and the Omagh bombing. If one imagines a situation emerging in the future which mirrored what occurred in the Graham Dwyer case, with the fact that a serious crime had been perpetrated only becoming known long after the crime had actually been committed, one can see immediately how disadvantaged criminal investigators would be.

4.88 Given that it is not possible to require service providers to retain traffic and location data to be available for criminal investigation, that places a premium on investigators to make requests at the earliest possible stage when there may still be hope that there will be data in existence which can be accessed through preservation and production orders.

4.89 The efforts in this regard of An Garda Síochána, in particular, to make the best of a bad situation are estimable. I am aware that members of the Security and Intelligence section working in the area have conducted a broad internal information campaign, addressing investigators with a view to getting across the message that there may still be cases where worthwhile results can be achieved, but for that to happen, it is imperative that the need to access data be identified at the earliest possible stage and then acted upon.

Independence of Senior Officers Receiving Applications for Cell Site Data

4.90 There is stipulation in a number of places in the legislation that whenever an application is made to a superior officer, that superior officer must not have had any prior involvement in the matter.

4.91 In the case of applications for cell site data for the purpose of protecting the life or personal safety of a person, where the member believes there is a serious risk to the life or personal safety of the person, or for the purpose of determining the whereabouts of a missing person, I believe that the exclusion of superior officers with prior involvement adds little and introduces an unnecessary complication. I therefore recommend that consideration should be given to providing for exceptions to this requirement in these cases.

SUMMARY OF RECOMMENDATIONS – 2011 ACT

Expressly and directly provide for powers under this Act for the Police Ombudsman in statute.

Consider amending the legislation to provide for exceptions to the requirement that authorisations for cell site data for the purpose of protecting the life or personal safety of a person or for the location of a missing person may not be made by a senior officer having any prior involvement.

5

The Year Ahead

Categories of Particular Sensitivity

5.1 The McCullough Report[47] was published in September 2025 and was conducted against a background of concerns about surveillance of journalists and lawyers by the PSNI. Having read the report, which found that there was no evidence of systemic and widespread surveillance, but which did report instances of concerning activity by the police, I made a decision to raise the topic with each of the bodies exercising intrusive powers.

5.2 Specifically, I asked each body to consider whether their application process reflected the recognition of the added sensitivity involved in cases where categories of privilege may exist. These include cases where the action proposed would likely have implications for legal professional privilege, journalistic privilege or other areas of particular sensitivity, such as membership of the Oireachtas. In such cases, likely to be rare, there should be specific consideration given at an appropriately high level to the question of whether the action contemplated is nonetheless appropriate and proportionate.

5.3 My recommendation to the authorised bodies was to specifically include and record in their internal procedural documents whether:

- particular sensitivities apply to the exercise of the intrusive powers in each application, and
- if such sensitivities or categories of privilege exist, that appropriate consideration has been given in assessing the proportionality of the application.

This suggestion was well received by all relevant bodies.

5.4 I should make clear that my decision to raise the topic was not based on any concern that statutory powers had been exercised inappropriately. Rather, I believed that embedding consideration of categories of particular sensitivity in the standard internal application process and documenting that the issue had been addressed in a satisfactory manner would represent a worthwhile safeguard.

5.5 My next round of review visits covering the first quarter of 2026 will take place over Easter and I will include this as an item for discussion at those meetings.

47. Available at https://www.psni.police.uk/sites/default/files/2025-09/The%20McCullough%20Review.pdf [last accessed on 18 March 2026].

Reports

5.6 The coming months will see further work on the Criminal Justice (Terrorist Offences) Act 2005 and the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, with a view to reporting on these pieces of legislation as part of my next annual report.

5.7 I will also commence work on the Offences against the State Act 1939, but in circumstances where it was the subject of a recent review, the contents of which are the subject of consideration at government level, I do not at present envisage reporting on it in the course of the next annual report.

Engagement

5.8 Over the coming months, in the context of developing our Statement of Strategy and also our broader programme of work, I will extend contact with civil society, service providers and other stakeholders, particularly those with established expertise in the area, and seek their views.

Espionage

5.9 It is also my intention in the short term to carry out an overview of our existing espionage legislation to see whether a full review is warranted. I am minded to do this because our main legislation in this area, the Official Secrets Act 1963, dates from more than 60 years ago, and also because I am conscious that a number of other countries, including the United Kingdom and Australia, have recently conducted reviews resulting in legislative amendment.

SUMMARY OF RECOMMENDATIONS

Interception of Postal Packets and Telecommunications (Regulation) Act 1993

- Develop legislative basis for interception of and access to modern, digital communications.
- Provide legislative basis for lawful access to all communications, including encrypted communications, incorporating appropriate safeguards.
- Provide for secure storage and access in any amending or new legislation.
- Develop legislative basis for use of electronic scanning equipment that can locate and record identifier data from mobile devices.
- Broaden the scope of postal interception to include delivery and courier services beyond An Post.
- Develop an accelerated procedure to provide for situations of urgency.
- Address the apparent need for the Garda Commissioner to provide a physical signature.
- Examine potential models for prior judicial authorisation of interception applications.

Criminal Justice (Surveillance) Act 2009

- Provide for authorisation of tracking devices by superior officers on a short-term basis, with a requirement to seek judicial affirmation.
- Introduce legislative requirement for senior officers authorising urgent applications for surveillance or applications for tracking devices to be independent of the investigation or operation.
- Address the issue of the deployment of tracking devices after a period of four months' monitoring.
- Consider providing for longer periods of retention of surveillance material, with appropriately strict access restrictions.
- Make provision by Ministerial order for appropriate secure storage and restriction of access to surveillance material.

Communications (Retention of Data) Act 2011

- Expressly and directly provide for powers under this Act for the Police Ombudsman in statute.
- Consider amending the legislation to provide for exceptions to the requirement that authorisations for cell site data for the purpose of protecting the life or personal safety of a person or for the location of a missing person may not be made by a senior officer having any prior involvement.

PART 3

Culture and Governance

6

Culture and Behaviours

Mission and Values

6.1 The culture in the office of the Independent Examiner of Security Legislation is informed by our mission and shared values, which were developed in whole-team workshop sessions. These interactive discussions helped all staff to explore and come to a clear understanding of the functions of the organisation, as well as agreement on our priorities in carrying out our mandate responsibly and respectfully.

OUR MISSION

Our mission is to support the protection of the security of the State through independent oversight of security legislation.

We will promote public confidence in security legislation by seeking to ensure that it is effective, necessary and proportionate, and also safeguards human rights, civil liberties and due process.

OUR VALUES

We are guided by our core values: balance, respect and open-mindedness.

We will have no pre-conceptions in how we approach our work. We will listen and hear the views of all with an open mind.

Our reporting will be balanced and responsible, with the aim of supporting the security of the State, respecting human rights and serving the greater good.

6.2 Every member of staff is aware of the significance of our work, and of the personal integrity required of each individual in all we do and in our relationships with our partners and wider stakeholders.

6.3 The work of the OIE concerns matters of special sensitivity and often, information of a confidential and secret nature. The 2024 Act sets out the penalties for disclosure of sensitive information by a member of OIE staff, which exceed the penalties for disclosure of information in contravention of the Official Secrets Act 1963, both in the maximum fine amount or term of imprisonment. Every member of staff was made aware of this higher duty of confidentiality before being offered a position and this practice will continue for future recruits.

6.4 All members of staff are expected to abide by and support the principles and values set out in the Civil Service Code of Standards and Behaviour, as well as all policies and procedures in effect for civil servants of the Department of Justice, Home Affairs and Migration. All staff are provided with a link to these corporate and civil service policies and procedures on the Department's intranet.

6.5 All OIE staff members have completed formal training to improve familiarity with the Civil Service Code of Standards and Behaviour.

Commitment to the Protection of Human Rights and Equality

6.6 The protection of human rights and equality is central to the work of the office of the Independent Examiner of Security Legislation. One of the organisation's core functions, explicitly set out in statute, is to keep under review the operation and effectiveness of security legislation, including by examining whether it "contains sufficient safeguards for the protection of human rights" (section 234 (2)(a)(i)(II) of the Policing, Security and Community Safety Act 2024).

6.7 This particular function is the lens through which all reviews of the implementation of the intrusive powers are carried out. It has influenced the development of our culture and values as an organisation, and it is actively kept at the forefront of all the OIE's internal and external engagement.

6.8 The OIE is committed to fulfilling its public sector duty as set out in section 42 of the Irish Human Rights and Equality Commission Act 2014. From the pre-establishment phase, when designing the organisational structure of the agency, recruiting new team members and mapping out how the functions of the OIE might be put into practice, a key guiding principle in all decision-making was the creation of a culture of respect for human rights and equality among our team members and for the people we serve.

6.9 Within the first six months of operation, all OIE staff members completed training on the section 42 public sector duty. Further training on human rights or related equality matters is actively encouraged and will be supported and facilitated in line with the values and business needs of the organisation.

6.10 In the coming year, we will develop our first Public Sector Duty Assessment and Action Plan. The consultation process with team members, stakeholders and members of the public will help us to better understand the equality and human rights issues that matter to people, areas where we can do better and issues we should consider, so that we can ensure that we continue to improve. In line with our core values of balance, respect and open-mindedness, we will listen to all views without prejudice or preconception and these will contribute to the public sector duty goals we set for ourselves.

6.11 As an organisation, we are keenly aware of the Independent Examiner's statutory objective of promoting public confidence in security legislation. We believe that this involves both seeking assurance that the human rights of all are protected in security legislation and its implementation, along with reporting on this to the greatest extent possible, without prejudicing the security of the State, defence or international relations. The inspection of individual files in the quarterly review visits includes checking that each authorised body has applied the appropriate tests of proportionality, duly considered potential collateral intrusion, assessed whether less intrusive measures might achieve the desired objective and satisfied themselves that use of security legislation provisions in every individual case was only considered when deemed absolutely necessary and in line with a clear strategic objective.

6.12 As new situations and threats emerge, and with the rapid advance of technology and communications, it is likely that legislation will be introduced or amended to keep pace and support the State in countering threats to the security of its people. In fulfilling its statutory mandate to review the operation and effectiveness of security legislation and services, the office of the Independent Examiner will ensure that the focus on human rights remains consistent and keeps up with the complex and ever-evolving security landscape.

7

Governance

Financial and Risk Management

7.1 The office of the Independent Examiner is a statutory agency funded under the Department of Justice, Home Affairs and Migration Vote (Vote 24), for which the Department's Secretary General is Accounting Officer. The OIE is supported by the shared financial service provided by the Department.

7.2 The Head of Office (Principal Officer) is responsible for the day-to-day management of the OIE's budget, preparation of the annual estimates documents and engagement with the Department on finance and procurement-related matters. Monthly expenditure reports assist in monitoring the OIE's management of its financial resources.

7.3 The Financial Shared Services Centre of the Department processes a range of financial services on behalf of the OIE, including the payment of salaries, invoices and travel & subsistence.

Procurement

7.4 The Office of the Independent Examiner is aware of its obligations to comply with national and EU policies in respect of procurement, together with the delivery of value for money. The OIE operates in accordance with the general departmental rule on procurement whereby the value of a contract determines the procurement route.

Audit and Risk

7.5 The office of the Independent Examiner has carried out an assessment of its principal risks and has put a risk management system in place, which:

- Identifies risks that are strategic in nature and/or have the significance to impact on the organisation as a whole and
- Includes a risk register which identifies the key risks facing the OIE, assesses the likelihood of each risk occurring, and puts in place controls for the mitigation and management of risk.

7.6 The OIE team meets weekly. In the first team meeting of every month, the Risk Register is reviewed to:

- Add new risks identified by staff;
- Consider the ranking and mitigation of risks;
- Escalate or decrease the ratings of particular risks in light of changing circumstances.

The outcome of these assessments is used to plan and allocate resources to ensure risks are managed to an acceptable level.

7.7 As a smaller body funded under the Justice Vote (Vote 24), the OIE does not currently have its own internal audit function or audit committee. The Department's Internal Audit Unit (IAU) supports the OIE in monitoring and reviewing the effectiveness of its arrangements for internal governance, risk management and internal control.

Adherence to Governance Codes and Standards

Statutory and Other Corporate Governance Obligations

7.8 The office of the Independent Examiner is subject to a range of statutory and other corporate governance obligations including the applicable provisions of the Code of Practice for the Governance of State Bodies, the Corporate Governance Standard for the Civil Service and relevant circulars and guidance.

7.9 The Head of Office is responsible for ensuring compliance with all relevant obligations.

Corporate Governance Assurance Agreement

7.10 In accordance with the Code of Practice for the Governance of State Bodies (2016), the Department of Justice, Home Affairs and Migration has drawn up a Corporate Governance Assurance Agreement in consultation with the office of the Independent Examiner of Security Legislation.

7.11 This Agreement covers the period 2026-2028 and sets out the broad governance and accountability framework within which the office of the Independent Examiner operates and defines the key roles and responsibilities which underpin the relationship between the OIE and the Department.

7.12 The Corporate Governance Assurance Agreement is published on the website of the office of the Independent Examiner, www.independentexaminer.ie.

Further Governance Obligations

Confidentiality

7.13 The office of the Independent Examiner is subject to a number of specific obligations which are detailed in the Policing, Security and Community Safety Act 2024.

7.14 The 2024 Act sets out requirements in relation to confidentiality, which places a higher duty of confidentiality on staff of the OIE than in most other areas of civil service employment. The penalties for reckless or intentional disclosure of sensitive information are listed in section 250 of the 2024 Act.

Security of information

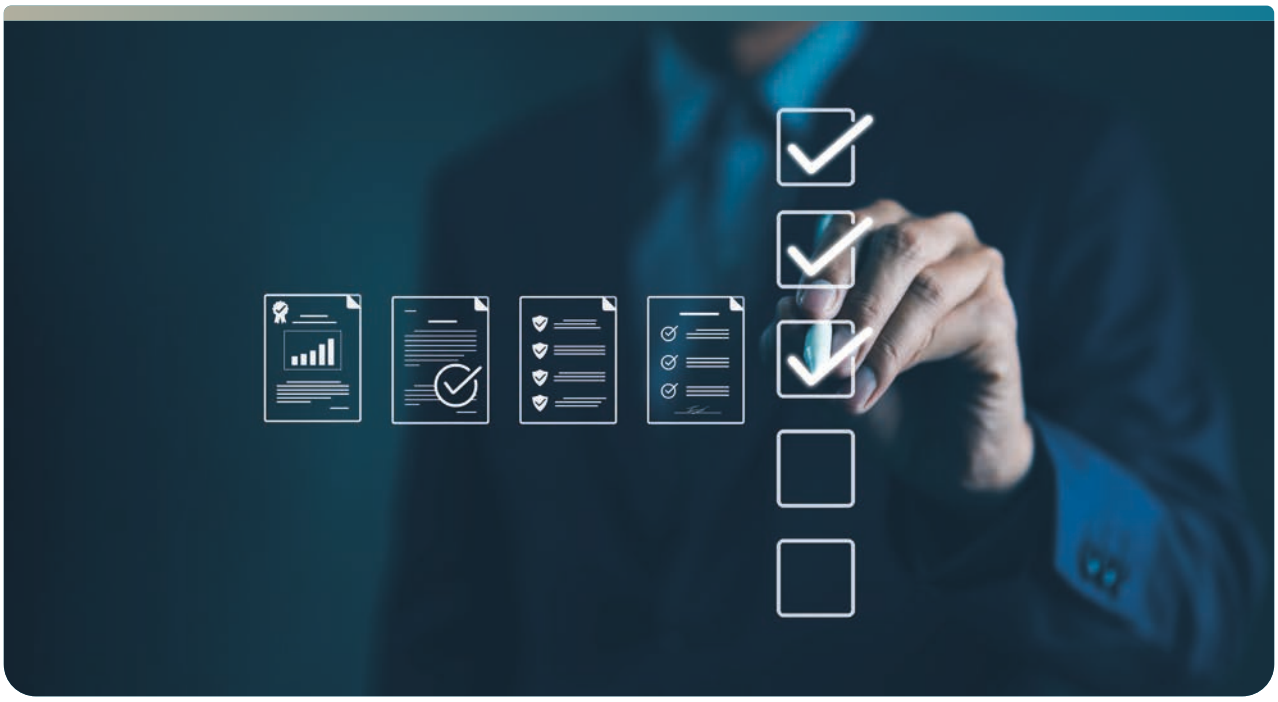
7.15 Section 251(1) of the 2024 Act describes the Independent Examiner's obligation to put in place *"...all necessary and reasonable measures to ensure the security of any information, document or thing provided to him or her or otherwise obtained by him or her in the course of performing his or her functions."*

7.16 The OIE continuously strives to meet this statutory obligation through a combination of physical security measures and standard operating procedures and practices aimed at avoiding and/or minimising risk and mitigating against its impact.

7.17 Further physical security measures are being developed in consultation with expert partners and include building security, equipment and cyber security. Where appropriate, elements are governed by internal policies, which are assessed regularly as part of the OIE's monthly risk review meetings.

7.18 Relevant work procedures and practices are designed to protect both information and staff members. They ensure consistency of practice and a high awareness among staff of the importance of safeguarding sensitive and confidential information.

7.19 It is important to note that I have given assurance to all relevant bodies that I intend to review all particularly sensitive material on-site at their secure locations and I have done this.



Freedom of Information

7.20 The Freedom of Information Act 2014 (FOI Act) confers a statutory right on all members of the public to access records held by public bodies including the office of the Independent Examiner of Security Legislation, while balancing the public interest and the right to privacy of individuals.

7.21 The office of the Independent Examiner of Security Legislation is a "partially included agency" under the FOI Act. This means that Freedom of Information requests may be submitted only in relation to the general administration of the office.

7.22 The FOI Act does not apply to records held or created by the Independent Examiner of Security Legislation. These Freedom of Information provisions are set out in section 292 of the Policing, Security and Community Safety Act 2024.

7.23 Anyone wishing to make a Freedom of Information request can email: foi@independentexaminer.ie.

Data Protection

7.24 The office of the Independent Examiner of Security Legislation is committed to protecting the rights and privacy of all individuals in accordance with the EU General Data Protection Regulation, 2016/679 (GDPR) as given further effect in Part 3 of the Data Protection Act 2018. Section 8 of the 2018 Act provides that the Data Protection Act 1988 will continue to govern the processing of personal data for the purposes of safeguarding the security of the State, the defence of the State or the international relations of the State.

7.25 The Data Protection Officer for the Department handles data protection matters for the OIE and can be contacted at dataprotectioncompliance@justice.ie.

Provision of Information to Members of the Oireachtas

7.26 The OIE has a dedicated email address for information requests from Oireachtas Members, oireachtas@independentexaminer.ie, in line with Circular 25/2016 and the Code of Practice for the Governance of State Bodies, 2016. The OIE endeavours to respond to all correspondence as soon as possible and while the office has established a maximum target timeframe of 10 working days for general correspondence, requests from Oireachtas Members are prioritised.

Protected Disclosures

7.27 A protected disclosure is a disclosure of information which, in the reasonable belief of a worker, tends to show one or more relevant wrongdoings that came to the attention of the worker in a work-related context and is disclosed in the manner prescribed in the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022.

7.29 The Protected Disclosures Act protects workers from penalisation if they speak up about relevant wrongdoing in the workplace. Persons who make protected disclosures (sometimes referred to as "whistleblowers") are protected by this law.

7.29 The office of the Independent Examiner of Security Legislation operates under the Department of Justice, Home Affairs and Migration's Protected Disclosures Policy, which has been communicated to all staff and which set outs the process for any worker or former worker wishing to report a relevant wrongdoing.

Health and Safety

7.30 In advance of establishment, health and safety training was sought to enable the office of the Independent Examiner to develop a detailed Health and Safety Statement and a thorough Health and Safety Risk Assessment, ensuring compliance with best practice standards and legislative requirements as set out in the Safety, Health and Welfare at Work Act 2005.

7.31 In addition, selected staff members completed first-aid training, so that there is nearly always a trained first-aid responder on site to manage potential incidents. While this is sometimes a challenge with a small team, the planning of the weekly blended working schedule takes into account first aid cover.

Our Green Mission

7.32 As the office of the Independent Examiner of Security Legislation was established in April 2025, the organisation's baseline period for the 2030 targets will be 2026, the organisation's first full calendar year in existence.

7.33 The basis for the organisation's 2030 targets will be:

- a 9.5% improvement in energy efficiency by 2030, compared to the 2026 baseline period. (The target for longstanding public bodies is a 50% improvement by 2030, compared to a 2009 baseline), and
- a 17% reduction in fossil CO2 by 2030, compared to the 2026 baseline period. (The target for longstanding public bodies is a 51% reduction by 2030, compared to a 2016-2018 baseline).

7.34 The premises is powered by both electricity and gas. Given the short period of time the OIE has occupied its premises, a more comprehensive analysis will be carried out and baseline established over the coming year. It should be noted that 87 St Stephen's Green is a historical building and is listed on Dublin City Council's Record of Protected Structures. As a result, there are some restrictions on modifications that might alter the character, appearance or heritage of the building, which may limit some potential future interventions that could improve energy efficiency.

7.35 We will continue to engage with the Sustainable Energy Authority of Ireland (SEAI) and report into its Public Sector Monitoring and Reporting platform to determine our energy performance and greenhouse gas status and targets.

8

Strategic Vision

8.1 The establishment of the office of the Independent Examiner of Security Legislation marks a significant milestone in national security oversight in Ireland. The office provides, for the first time in the State, a dedicated and unified oversight role over security legislation and security services.

8.2 The office will embrace its statutory mandate to deliver independent, rigorous, transparent and rights-respecting scrutiny of security legislation and security services in the State. Over the next three years, we aim to build a strong foundation of expert oversight, public confidence and continuous learning, ensuring that as security challenges evolve, the State's security legislation and security services remain effective, necessary and proportionate to the protection of human rights.

8.3 Below, we have set out our key strategic goals for the next three years, with a view to conducting a comprehensive consultation process in 2026 and developing our formal Statement of Strategy.

8.4 Our main strategic goals over the next three years are to:

1. Explain what we do

8.5 **Explain the role of the OIE to our stakeholders and the public and ensure that information relating to our work is made available to the greatest extent possible, without prejudicing the security of the State, defence or international relations.**

8.6 As a new body, we want to ensure that our stakeholders and the public know about our role, including our objectives, functions and powers. We will achieve this strategic goal through continual updating of our accessible website, which provides comprehensive information about our work, through our reporting on security legislation and security services, and through engagement with our stakeholders. This will help to build understanding of our role and encourage informed public debate on security legislation and services.

2. Build relationships

8.7 **Build robust and collaborative relationships with our stakeholders, counterparts, civil society groups and experts in academia and practice.**

8.8 To achieve this goal, the OIE will continue to develop collaborative relationships based on mutual trust with relevant stakeholders engaged in the fields of national security and human rights. We will maintain and grow structured liaison mechanisms with our stakeholders to ensure effective information-sharing. Engagement with counterparts in other jurisdictions and civil society groups - particularly those working in human rights, civil liberties and privacy rights - will form a core part of our approach, enabling us to benefit from external insights and experience, identify emerging concerns, and ensure that diverse perspectives inform our scrutiny.

8.9 We will also cultivate strong connections and collaborations with experts in academia and practice in fields such as national security law, constitutional and administrative law, criminal law and criminology, the law of evidence and technology. We will draw on appropriate research and expertise to enhance the quality and contextual depth of our reports and reviews.

8.10 In doing so, we hope to encourage an open, informed dialogue on security legislation and services, and to establish the OIE as a trusted, accessible and authoritative voice for independent oversight within the national security framework of the State.

3. Promote public confidence

8.11 **Promote public confidence in security legislation and services by ensuring our reports and reviews are rigorous, fair, transparent and timely.**

8.12 In our reports and reviews, we aim to meet the highest standards of analytical rigour, fairness and transparency. Our work will be evidence-based and grounded in robust legal analysis. We will apply transparent methodologies so that our findings are understandable and credible, while clearly explaining any limitations or redactions required to protect the security of the State, defence or international relations.

8.13 The OIE commits to ensuring that our reports are planned, prepared and submitted to the Taoiseach within the timeframe set by legislation. Similarly, we will ensure that our reviews are completed in as timely a manner as possible.

4. Anticipate and respond

8.14 **Anticipate and respond effectively to an evolving security and oversight environment.**

8.15 The OIE will adopt a forward-looking approach that seeks to identify emerging security threats, technological developments and societal changes with potential implications for security legislation and oversight. This will involve systematic monitoring of national, European and international trends in areas such as interception of communications, access to data, surveillance, artificial intelligence, terrorism, espionage, state threats and transnational organised crime. The OIE will engage with our stakeholders and counterparts and draw on academic and practitioner expertise to assess whether existing legislative frameworks remain fit for purpose and proportionate. Where risks or gaps are identified, the OIE will highlight these in our reporting, thereby helping to support early, evidence-based consideration of legislative or policy reform.

8.16 By embedding a horizon-scanning approach into our strategic planning and review functions, the OIE aims to support the proportionate and rights-respecting operation of security legislation and security services on a long-term and sustainable basis.

8.17 This will require building capacity, expertise and institutional knowledge within the organisation, to further develop a robust and agile agency that can fulfil its statutory mandate in an evolving and increasingly complex security landscape.

8.18 Through these measures, the OIE will promote public knowledge and confidence, strengthen accountability and ensure that our work contributes to a long term, effective, transparent and rights-protective framework for security oversight.

Notes

Notes

Notes

Oifig an Scrúdaitheora
Neamhspleách um
Reachtaíocht Slándála

Office of the Independent
Examiner of Security Legislation

www.independentexaminer.ie