Short Thematic Report

National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

Legal update

Country: Ireland

Version of 29 June 2016

FRANET contractor: Irish Centre for Human Rights, National University of Ireland, Galway

Author(s) name(s): Dr. TJ McIntyre

1 Description of tasks – Phase 3 legal update

1.1 Summary

*FRANET contractors are requested to highlight in 1 to 2 pages **maximum** the key developments in the area of surveillance by intelligence services in their Member State. This introductory summary should enable the reader to have a snap shot of the evolution during the report period (last trimester of 2014 until mid-2016). It should in particular mention:*

1. *the legislative reform(s) that took place or are taking place and highlight the key aspect(s) of the reform.*
2. *the important (higher) court decisions in the area of surveillance*
3. *the reports and inquiry by oversight bodies (parliamentary committes, specialised expert bodies and data protection authorities) in relation to the Snowden revelations*
4. *the work of specific ad hoc parliamentary or non-parliamentary commission (for example the NSA inquiry of the German Parliament) discussing the Snowden revelations and/or the reform of the surveillance focusing on surveillance by intelligence services should be referred to.*

Preliminary observations

It may be useful to begin by recalling the fact that Ireland does not have a distinct intelligence agency – intelligence and state security functions are the responsibility of the Garda Síochána (police force) and Defence Forces.[1] There is therefore no rigid dividing line between intelligence and law enforcement surveillance – for the most part the same powers will apply in both contexts. Consequently while many of the updates in this report primarily relate to law enforcement surveillance they will also be relevant to intelligence surveillance. For the same reason, there is no distinct legal basis for intelligence functions and portions of this draft report may therefore have to be slightly longer than requested in order to explain how the intelligence functions fit into the wider Garda Síochána and Defence Forces surveillance framework, and how their application differs from surveillance and information sharing in a criminal justice context.

Legislative reforms

No new legislation in relation to surveillance was enacted in Ireland during the reporting period. However, an existing provision – Part 3 of the Criminal Justice (Mutual Assistance) Act 2008 – was brought into force in December 2014.[2] This implements the Convention on Mutual Assistance in Criminal Matters and provides for mutual assistance between Ireland and other EU Member States regarding interception of communications as part of criminal investigations. Controversially, it also permits prosecutions *in camera* (i.e. in secret) of telecommunications firms which fail to comply with ministerial directions in relation to surveillance.[3] This has been criticised on the basis that it may permit more invasive surveillance practices to develop outside public scrutiny.[4]

Court decisions in the area of surveillance

There have been no published decisions of the higher courts on surveillance during the reporting period. There was one *ex tempore* decision during this time (i.e. judgment was delivered orally and no written judgment given). In March 2015 an accused was convicted of murder in a case based in large part on retained telecoms data. He had challenged the admissibility of retained data in light of the *Digital Rights Ireland*[5] decision but the High Court held that notwithstanding that decision national data retention law remained valid and therefore the data was admissible.[6] That conviction, including the data retention issue, is currently under appeal.[7]

Reports and inquiries by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) in relation to the Snowden revelations

[1] See e.g. Mulqueen, M. (2008), 'A Weak Link? Irish National Security Policy on International Terrorism,' *Contemporary Security Policy* Vol. 28, No. 2, pp. 330–56.
[2] Criminal Justice (Mutual Assistance) Act 2008 (Commencement) Order, S.I. No. 541/2014.
[3] Section 30 of the Criminal Justice (Mutual Assistance) Act 2008.
[4] Lillington, K., 'State Sanctions Phone and Email Tapping,' *The Irish Times*, December 6, 2014, available at: http://www.irishtimes.com/business/technology/state-sanctions-phone-and-email-tapping-1.2027844; Lillington, K., 'Surveillance by a Government-Sponsored Secret System,' *Irish Times*, December 11, 2014, available at: http://www.irishtimes.com/business/technology/surveillance-by-a-government-sponsored-secret-system-1.2033443.
[5] Court of Justice of the European Union, joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014.
[6] Gartland, F., 'Dwyer Appeal Likely to Focus on Phone Data and Questioning,' *The Irish Times*, May 31, 2015, available at: http://www.irishtimes.com/news/crime-and-law/courts/criminal-court/dwyer-appeal-likely-to-focus-on-phone-data-and-questioning-1.2159181; Mac Cormaic, R. and Gartland, F., 'Graham Dwyer Appeal May Be Heard by End of Year,' *The Irish Times*, May 11, 2015, available at: http://www.irishtimes.com/news/crime-and-law/graham-dwyer-appeal-may-be-heard-by-end-of-year-1.2207729.
[7] Gartland, 'Dwyer Appeal Likely to Focus on Phone Data and Questioning'; Mac Cormaic and Gartland, 'Graham Dwyer Appeal May Be Heard by End of Year.'

Parliamentary committees

There have been no parliamentary inquiries in Ireland in relation to Snowden, despite his revelations that fibre-optic cables to Ireland are specifically targeted by the UK agency GCHQ[8] and the fact that Dublin is home to the European headquarters of many of the internet firms involved in those disclosures.[9]

Data protection authorities

An investigation prompted by the Snowden revelations is currently being carried out by the Data Protection Commissioner ("DPC"). This originated in complaints by Max Schrems regarding the transfer of data by Facebook to the United States, challenging the adequacy of data protection in the United States in light of the PRISM program exposed by Snowden.[10] These complaints were initially dismissed by the DPC as "frivolous and vexatious" on the basis that the DPC had no power to look behind the Commission's determination of adequacy in the Safe Harbor decision. As is well known, Mr. Schrems judicially reviewed this decision of the DPC and on a preliminary reference the Court of Justice of the European Union ("CJEU") found that the Safe Harbor decision was invalid and that national data protection authorities were bound to investigate complaints regarding transfer of data to third countries even where a Commission finding of adequacy is in place.[11] Following this ruling, in October 2015 the High Court quashed the decision of the DPC refusing to investigate Mr. Schrem's complaint and the DPC undertook to investigate the complaint speedily.[12]

As part of this investigation, in May 2016 the DPC issued a preliminary decision that the transfer of data by Facebook to the United States could not be validated by the use of model contract clauses.[13] The preliminary decision found that such transfers are likely to breach the Charter of Fundamental Rights on the basis that EU citizens do not have an adequate remedy in the US where their data may be at risk of being accessed by US state agencies for national security purposes in a manner incompatible with the Charter. The DPC has now issued proceedings in the Irish High Court which seek to have the matter referred to the CJEU for a ruling on the legal status of data transfers under such clauses.[14] In an unprecedented development, the United States government has applied to the court for permission to take part in these proceedings as an amicus curiae.[15]

While this is a significant case, as highlighted by the involvement of the US government, it should be noted that it is primarily an investigation of data transfers between the Facebook Irish and US corporate entities – while the legality of these transfers may depend on US surveillance

[8] Sheridan, G., Kelly, F., and McManus, J., 'UK Spy Base GCHQ Tapped Irish Internet Cables,' *The Irish Times*, November 29, 2014, available at: http://www.irishtimes.com/business/technology/uk-spy-base-gchq-tapped-irish-internet-cables-1.2019492; McIntyre, T.J., 'Why Ireland Must Protect Privacy of Irish Emails and Internet Usage from Surveillance,' *The Irish Times*, December 20, 2014, available at: http://www.irishtimes.com/opinion/why-ireland-must-protect-privacy-of-irish-emails-and-internet-usage-from-surveillance-1.2044384.

[9] McIntyre, T.J., 'Ireland,' in *A Crisis of Accountability: A Global Analysis of the Impact of the Snowden Revelations*, ed. Davies, S. (IViR / LSTS, 2014), available at: http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf.

[10] See *Schrems v. Data Protection Commissioner* [2014] IEHC 310.

[11] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, judgment of 6 October 2015.

[12] Carolan, M., 'Data Protection Commissioner to Investigate Max Schrems Claims,' *The Irish Times*, October 20, 2015, available at: http://www.irishtimes.com/news/crime-and-law/courts/high-court/data-protection-commissioner-to-investigate-max-schrems-claims-1.2398728.

[13] Schrems, M., 'Facebook & NSA-Surveillance: Following 'Safe Harbor' Decision, Irish Data Protection Commissioner to Bring EU - US Data Flows before CJEU Again,' *Europe v. Facebook*, May 25, 2016, available at: http://www.europe-v-facebook.org/PA_MCs.pdf.

[14] Robinson, D., 'Ireland Warns on Big Tech's Data Rules,' *Financial Times*, May 25, 2016, available at: http://www.ft.com/fastft/2016/05/25/ireland-warns-on-big-techs-data-rules/.

[15] Carolan, M., 'US Government Wants to Be Joined in Schrems Case,' *The Irish Times*, June 13, 2016, available at: http://www.irishtimes.com/business/technology/us-government-wants-to-be-joined-in-schrems-case-1.2683066.

laws as applied to Facebook, it is nevertheless not an investigation of wider US surveillance practices and of course does not address Irish surveillance practices.

Work of specific ad hoc parliamentary or non-parliamentary commissions discussing the Snowden revelations

There have been no official commissions examining the Snowden revelations.

Work of specific ad hoc parliamentary or non-parliamentary commissions discussing reform of surveillance, focusing on surveillance by intelligence services

In January 2016, following political controversy regarding a police oversight body accessing journalists' phone records to investigate leaks, the Government appointed a retired judge to carry out an independent review of the law in this area.[16] The terms of reference of the review are as follows: "To examine the legislative framework in respect of access by statutory bodies to communications data of journalists held by communications service providers, taking into account, the principle of protection of journalistic sources, the need for statutory bodies with investigative and/or prosecution powers to have access to data in order to prevent and detect serious crime, and current best international practice in this area".[17] These terms are wide enough to cover access for intelligence purposes. This review has not yet reported.

Statistics

The availability of statistics depends on the nature of the surveillance involved.

The Department of Justice has refused to provide statistics on the number of warrants issued for the interception of communications on the basis that to do so would undermine national security or the investigation of serious crime.[18] It has also refused to allow individual telecommunications providers to publish such information as part of their transparency reports, despite the lack of any legal basis for such a prohibition.[19]

There is considerably more transparency in relation to surveillance under the Criminal Justice (Surveillance) Act 2009 (generally audio bugs, covert videos and tracking devices) where the designated judges appointed under that Act have provided detailed statistics in their annual reports.[20] In 2015, for example, the report indicated that the Garda Síochána had been given 37 court authorisations to use surveillance devices and had given internal approval for the use of two devices in cases of urgency. Tracking devices were used by police in 12 cases.[21]

The position in relation to statistics on data retention and access to telecommunications data is in a state of flux. The Department of Justice historically refused to provide any figures on the

[16] Griffin, D., Minihan, M., and Bardon, S., 'Retired Chief Justice Appointed to Examine Phone Records Law,' *The Irish Times*, January 19, 2016, available at: http://www.irishtimes.com/news/crime-and-law/retired-chief-justice-appointed-to-examine-phone-records-law-1.2502099.

[17] 'Statement by the Minister for Justice and Equality in Relation to Access to Telephone Records,' January 19, 2016, available at: http://merrionstreet.ie/en/News-Room/Releases/Statement_by_the_Minister_for_Justice_and_Equality_in_relation_to_access_to_telephone_records.html.

[18] MacGuill, D., 'State Surveillance: What the Government and Gardaí Don't Want You to Know,' *TheJournal.ie*, May 17, 2015, available at: http://www.thejournal.ie/ireland-state-surveillance-wiretapping-gardai-crime-transparency-2105584-May2015/.

[19] Horgan-Jones, J., 'Only One Country Refused to Allow Vodafone Publish Spying data…Ireland,' *TheJournal.ie*, June 6, 2014, available at: http://www.thejournal.ie/vodafone-government-refusals-makey-uppy-law-1502972-Jun2014/.

[20] These reports are available at Digital Rights Ireland, 'Surveillance Library,' accessed March 25, 2015, available at: https://www.digitalrights.ie/irish-surveillance-documents/.

[21] McCárthaigh, S., 'State Snooping Works, High Court Judge Says,' *The Times*, March 11, 2016.

use of data retention.[22] Until its invalidation in 2014 the Data Retention Directive[23] enforced a degree of transparency by requiring annual reports by Member States to the Commission which then published the statistics for each country.[24] However, since the invalidation of the Directive the State seems to have reverted to its earlier position of secrecy and the Garda Síochána has refused to release information as to how often it has accessed telecommunications records.[25] It is possible for individual telecommunications firms to disclose the number of requests they receive for communications data; however, so far only one provider – Vodafone – has done so.[26]

1.2 International intelligence services cooperation

*FRANET contractors are requested to provide information, in 1 to 2 pages **maximum**, on the following two issues, drawing on a recent publication by Born, H., Leigh, I. and Wills, A. (2015), Making international intelligence cooperation accountable, Geneva, DCAF.*[27]

1. *It is assumed that in your Member State international cooperation between intelligence services takes place. Please describe the legal basis enabling such cooperation and any conditions that apply to it as prescribed by law. If the conditions are not regulated by a legislative act, please specify in what type of documents such cooperation is regulated (e.g. internal guidance, ministerial directives etc.) and whether or not such documents are classified or publicly available.*
2. *Please describe whether and how the international cooperation agreements, the data exchanged between the services and any joint surveillance activities, are subject to oversight (executive control, parliament oversight and/or expert bodies) in your Member States.*

[22] 'Parliamentary Question on Data Retention,' *Digital Rights Ireland*, October 25, 2005, available at: https://www.digitalrights.ie/parliamentary-question-on-data-retention/.
[23] Directive 2006/24/EC.
[24] Article 10. This is reflected in section 9 of the Communications (Retention of Data) Act 2011.
[25] Lally, C. and Bardon, S., 'Majority of 62,000 Data Requests Made by Garda,' *The Irish Times*, January 20, 2016, available at: http://www.irishtimes.com/news/crime-and-law/majority-of-62-000-data-requests-made-by-garda-1.2503021.
[26] Vodafone, 'Vodafone Law Enforcement Disclosure Report: Legal Annexe,' June 2014, available at: http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf; Lillington, K., 'Hurrah for Vodafone, Boo for the Government,' *The Irish Times*, June 12, 2014, available at: http://www.irishtimes.com/business/technology/hurrah-for-vodafone-boo-for-the-government-1.1829002; Pope, C., 'Vodafone Report Sparks Interception Law Concerns,' *The Irish Times*, June 7, 2014, available at: http://www.irishtimes.com/news/consumer/vodafone-report-sparks-interception-law-concerns-1.1823901.
[27] http://www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable

Please describe the legal basis enabling such cooperation and any conditions that apply to it as prescribed by law.

The Irish government has on a number of occasions confirmed that extensive intelligence sharing takes place between the Garda Síochána[28], Defence Forces[29] and overseas intelligence agencies.[30] However – unlike international cooperation in the criminal law where there are a number of governing legal instruments[31] – there is no explicit legislative basis regulating cooperation with other intelligence services and there is no publicly available information regarding any internal documents, regulations or guidelines governing such cooperation.

This lack of an explicit legal basis reflects the absence of any distinct intelligence service and in particular the lack of a separate foreign intelligence service. As noted by one leading academic "[a]though domestic intelligence has always been a central component of Irish security, Ireland has apparently refrained from developing a foreign intelligence of its own… Covert (and, after 1985, overt) security cooperation with Western intelligence has apparently proved sufficient in this regard".[32]

Because there is no specific law or public guidance in this area it is difficult to give a definite answer as to what conditions apply in practice. However it would seem that intelligence sharing takes place on a largely discretionary basis. For example, consider material gathered by the use of audio bugs planted under the Criminal Justice (Surveillance) Act 2009. The 2009 Act imposes a general obligation of confidentiality in respect of such material – however, it goes on to provide that the Commissioner of the Garda Síochána and/or the Chief of Staff of the Defence Forces may authorise disclosure of that information to any person (which would include foreign intelligence services) "in the interests of the security of the State".[33] The 2009 Act does not impose any other criteria to be met before such material may be shared, nor does it impose any restrictions on how such information may be used by third parties. A similarly wide power to share exists in respect of intercept material, which permits such material to be disclosed so far as "necessary… in the interests of the security of the State" but without otherwise imposing any controls on dissemination to other intelligence services.[34]

Please describe whether and how the international cooperation agreements, the data exchanged between the services and any joint surveillance activities, are subject to oversight (executive control, parliament oversight and/or expert bodies) in your Member States.

In general, the Garda Síochána is answerable to the Minister for Justice and the Defence Forces to the Minister for Defence in respect of their surveillance and international cooperation

[28] See e.g. 'Government Statement on Terrorist Attacks in Brussels,' March 22, 2016, available at: http://www.merrionstreet.ie/en/News-Room/News/Government_Statement_Terrorist_Attacks_in_Brussels_22_March_2016.html.

[29] See e.g. Alan Shatter, Minister for Justice and Equality: 'The Defence Forces Intelligence Branch provide regular assessments, reports and briefings to the Chief of Staff, the Minister for Defence and the Secretary General of the Department of Defence, relating to internal or external threats to the security of the State and to national interests. Intelligence led liaison is conducted between Intelligence Branch and national authorities in other countries to counter any threat to the security of the State'. *Dáil Debates*, Written Answers, 18 June 2013.

[30] See also O'Halpin, E. (2002), 'Ireland and EU Intelligence Assessment: The Politics of an Undeclared Petersberg Task,' *Irish Political Studies* 17, No. 2, pp. 35–58; Mulqueen, 'A Weak Link?'

[31] For example, section 28 of the Garda Síochána Act 2005 permits the Garda Commissioner to 'enter into an agreement with a police service or other law enforcement agency outside the State… [which] may provide for the co-operation of the parties or the exchange of information or such other matters as the Garda Commissioner thinks fit'. Similarly, the Europol Act 2012 provides for the application of data protection law to activities related to Europol and designates the Data Protection Commissioner as the national supervisory authority.

[32] Jackson, P. (2000), 'Searching for Threats: Intelligence and Security in the Making of Modern Ireland,' *Irish Studies in International Affairs* 11, pp. 252–253; See also Mulqueen, 'A Weak Link?'

[33] Section 13 of the Criminal Justice (Surveillance) Act 2009.

[34] Section 12 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

activities which are carried out for the purposes of state security.[35] There is no Irish parliamentary or independent body oversight of these functions, so in practice these functions are only controlled by executive oversight.

It should be noted that amending legislation in 2015 made the Garda Síochána subject to an independent Policing Authority in respect of its policing services.[36] However, the remit of that body specifically excludes "security services", defined widely to include those functions that are concerned with "protecting the security of the State", "identifying foreign capabilities… that impact on the international or economic well-being of the State", and "co-operating with authorities in other states and international organisations".[37] In relation to state security and international cooperation, the Garda Síochána therefore remains answerable to the Minister for Justice only.

In relation to surveillance activities themselves, any joint surveillance will in principle be subject to the ordinary authorisation systems where the type of authorisation required differs depending on the nature of the surveillance. Interception of communications is authorised by a warrant from the Minister for Justice[38], the use of "surveillance devices" such as audio bugs and covert video cameras must generally be authorised by a District Court judge[39], while tracking devices can be planted[40] and retained communications data accessed[41] based on internal authorisation from a superior officer only. The use of informants or "covert human intelligence sources" is not regulated by statute and is subject to administrative approval only.[42] The use of "open source" or publicly available information (such as data-mining or profiling based on social media) does not appear to be subject to any particular statutory or administrative regulation.[43]

Oversight of surveillance is the responsibility of two separate "designated judges", who are High Court judges nominated by the President of the High Court.[44] One has responsibility for oversight of interception of communications and access to retained communications data[45], the other, responsibility for oversight of the use of "surveillance devices" and tracking devices.[46] In each case, the role of the designated judge is to keep the operation of the legislation under review, ascertain whether the authorities are complying with its provisions and provide an annual report to the Taoiseach (Prime Minister) including such matters as they think appropriate. However, in each case the role of the designated judge is limited to examining the

[35] See generally the Garda Síochána Act 2005 (as amended) and the Defence Act 1954 (as amended).
[36] See generally the Garda Síochána (Policing Authority and Miscellaneous Provisions) Act 2015.
[37] Section 4 of the Garda Síochána (Policing Authority and Miscellaneous Provisions) Act 2015.
[38] Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.
[39] Section 5 of the Criminal Justice (Surveillance) Act 2009.
[40] Section 8 of the Criminal Justice (Surveillance) Act 2009.
[41] Section 6 of the Communications (Retention of Data) Act 2011.
[42] There is also a non-statutory system of oversight by a retired judge. See Campbell, L., 'Informers in Ireland: A Lack of Law?,' *Human Rights in Ireland*, May 10, 2013, available at: http://humanrights.ie/uncategorized/informers-in-ireland-a-lack-of-law/; 'Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources,' 2006, available at: https://www.digitalrights.ie/dri/wp-content/uploads/2014/07/Management-and-use-of-Covert-Human-Intelligence-Sources.pdf; Walsh, D. (2009), *Human Rights and Policing in Ireland: Law, Policy and Practice*, Dublin, Clarus Press, chap. 27.
[43] See e.g. the comments of the Minister for Justice reported in Brennan, E., 'Minister Confirms Existence of Garda 'Operation Mizen' for Policing Water Charge Protests,' *Newstalk.com*, October 8, 2015, available at: http://www.newstalk.com/reader/47.301/56846/0/.
[44] See generally McIntyre, T.J. (2016), 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective,' in *Judges as Guardians of Constitutionalism and Human Rights*, ed. Scheinin, M., Krunke, H., and Aksenova, M., Cheltenham, Edward Elgar.
[45] Section 8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993; sections 11 and 12 of the Communications (Retention of Data) Act 2011.
[46] Section 12, Criminal Justice (Surveillance) Act 2009.

surveillance itself – there is no statutory power to examine the later *use* of surveillance material or its *sharing* with other intelligence agencies.[47]

There is a complaints procedure in respect of interception of communications, surveillance devices, tracking devices and access to retained data where individuals may raise concerns with a Complaints Referee.[48] The Complaints Referee is empowered to investigate whether surveillance took place without the appropriate authorisation or approval and if so to recommend payment of compensation and direct the destruction of any information obtained as a result. As with the designated judges, however, this function is limited to investigation of the fact of surveillance and whether appropriate permission as granted – it would not permit investigation of intelligence sharing or other downstream use of information gathered as a result.

The Data Protection Commissioner has limited power to review surveillance and intelligence sharing for state security purposes where the Executive objects to such review. There is a general exclusion in Irish data protection legislation which provides that data protection law "does not apply to… personal data that in the opinion of the Minister [for Justice] or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State"[49] and this is coupled with specific exclusions elsewhere in the legislation. For example, any restrictions on the processing of personal data "do not apply if the processing is… in the opinion of a member of the Garda Síochána [of a certain rank] or an officer of the Permanent Defence Force [of a certain rank] and is designated by the Minister for Defence under this paragraph, required for the purpose of safeguarding the security of the State".[50]

Consequently, while the DPC has examined surveillance in the criminal justice context – for example, a 2014 audit of the Garda Síochána reviewed access to retained telecommunications data[51] – this power does not extend to the state security context if the Executive objects to its use. It does not appear that it could be used to examine international cooperation agreements, data sharing or joint surveillance with intelligence agencies in other jurisdictions unless the relevant body within the Executive were to acquiesce to its use.

The Office of the DPC has explained the practical application of these exclusions as follows in an email of 18 July 2016:

> "notwithstanding the exclusion in the Irish Data Protection Acts ("the Acts") that applies to personal data kept for the purpose of safeguarding the security of the State, the Irish DPC has powers under Section 10 of the Acts to inspect any organisation and to validate their reliance on exemptions in relation to processing restrictions, i.e. ensure there is evidence of a due diligence procedure and appropriate level of sign-off in relation to the processing. For example, in 2016, the Irish DPC made inspections of An Garda Síochána and the Irish Army in order to examine any requests that had been made to telcos under the 2011 Act. Where certain files were indicated to the DPC to be classified as relating to national security, the DPC was able to examine the existence of the file type and to confirm the level of sign-off within the organisation for the file. It is therefore the case that the DPC can effectively audit the procedures that surround the processing of personal data that purports to be for national security purposes and can make a determination of the frequency of use of this classification."

[47] See e.g. section 8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.
[48] Appointed under section 9, Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.
[49] Section 1(4) of the Data Protection Acts 1988 and 2003.
[50] Section 8 of the Data Protection Acts 1988 and 2003.
[51] Data Protection Commissioner, 'An Garda Síochána: Final Report of Audit,' March 2014, 61, available at: http://www.garda.ie/Documents/User/An%20Garda%20S%C3%ADoch%C3%A1na%20ODPC%20Report%20Final.pdf.

9

It would appear from this description that the DPC has a largely procedural role in reviewing the system for applying national security classifications, but no substantive power to look behind such classifications (to determine whether they have been appropriately applied) nor to assess how the information subject to such classification is being processed.

Finally, mention should be made of the Garda Síochána Ombudsman Commission ("GSOC"). This body has the power to investigate complaints regarding allegations of misbehaviour by a member of the Garda Síochána, meaning conduct which "constitutes an offence or a breach of discipline".[52] This power could, in principle, be used to investigate complaints of illegal surveillance by a member but would not permit an investigation of wider surveillance and intelligence sharing practices unless these constituted criminal offences or breaches of discipline. Since 2015 GSOC has has the power to carry out wider investigations of Garda "practices, policies and procedures", but only insofar as this is for the purpose of preventing or reducing complaints.[53] For that reason, this power would not appear to permit GSOC to investigate surveillance and intelligence practices.

1.3 Access to information and surveillance

*FRANET contractors are requested to summarise, in 1 to 2 pages **maximum**, the legal framework in their Member State in relation to surveillance and access to information.*
Please refer to the Global Principles on National Security and the Right to Information (the Tshwane Principles)[54] (in particular Principle 10 E. – Surveillance) and describe the relevant national legal framework in this context. FRANET contractors could in particular answer the following questions:

1. *Does a complete exemption apply to surveillance measures in relation to access to information?*
2. *Do individuals have the right to access information on whether they are subject to surveillance?*

Does a complete exemption apply to surveillance measures in relation to access to information?

Yes. Freedom of information legislation provides a complete exemption in this context. The Freedom of Information Act entirely excludes from its scope any "record held or created by the Garda Síochána that relates to any of the following… the Security and Intelligence Section… the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993… the Criminal Justice (Surveillance) Act 2009 [and] the Communications (Retention of Data) Act 2011".[55]

As regards surveillance records held or created by other state bodies, the Freedom of Information Act 2014 provides that disclosure *may* be refused if access to a record "could reasonably be expected to affect adversely… the security of the State"[56] and goes on to provide that disclosure *must* be refused in respect of certain state security records including "information that was obtained or prepared for the purpose of intelligence in respect of the security or defence of the State" and information shared in confidence with other states relating to security, defence and international relations.[57]

[52] Sections 82 and 87 of the Garda Síochána Act 2005.
[53] Section 10 of the Garda Síochána Amendment Act 2015, substituting section 106 of the Garda Síochána Act 2005.
[54] http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-10
[55] Section 42.
[56] Section 33(1).
[57] Section 33(4).

10

A Minister may issue a conclusive (non-reviewable) certificate that particular records – including records relating to surveillance – fall within these categories.[58] However, such certificates are not a prerequisite for the refusal of access: requests for information may be refused on these grounds without the need for any such certificate. There is no publicly available information on how many requests have been refused on these grounds or whether any ministerial certificates have been issued on these grounds.

Do individuals have the right to access information on whether they are subject to surveillance?

No. The exemptions discussed above in relation to freedom of information requests apply equally to requests by individuals for information about themselves, including requests asking whether they have been subject to surveillance.

[58] Section 34. See also *Campbell v. Minister for Justice, Equality and Law Reform* [2010] IEHC 197 confirming that a court will not look behind the reason given for the issue of a certificate.

11

1.4 Update the FRA report

FRANET contractors are requested to provide up-to-date information based on the FRA report on Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – mapping Member States' legal framework.

*Please take into account the **Bibliography/References** (p. 79 f. of the FRA report), as well as the **Legal instruments index – national legislation** (p. 88 f. the FRA report) when answering the questions.*

Except as specifically indicated below, all references to Ireland have been checked and are accurate and up to date. Given the unusual nature of the Irish system (compared to the wider European context) there were generally no Irish references which were helpful for the wider comparative analysis.

Introduction

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

1 Intelligence services and surveillance laws

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

1.1 Intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

1.2 Surveillance measures

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

1.3 Member States' laws on surveillance

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2 Oversight of intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*

   At p.47 it is stated that "In nine Member States (Belgium, Cyprus, France, Germany, Greece, Ireland, Italy, Poland, Lithuania), DPAs have limited powers over intelligence services".

   While the law in this area is not entirely clear, in Ireland there is the possibility for a complete exclusion of information relating to state security from the area of data protection law which means that the DPC has no *compulsory* oversight power over the intelligence function.

   As already noted, under section 1(4) of the Data Protection Acts 1988 and 2003 Irish data protection law – including the oversight role of the DPC – "does not apply to… personal data that in the opinion of the Minister [for Justice] or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State". Consequently, while the DPC has a possible power to review the use of personal data in this context, that power is essentially subject to the consent of the executive – either the Minister for Justice or the Minister for Defence can in effect veto the exercise of that power. As discussed in section 1.2, the DPC has the power to examine the system by which information is classified in this way – but no power to review the use of such information.

   The same point can be made regarding the summary chart on p.49.

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.1 Executive control

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.2 Parliamentary oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.2.1 Mandate

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.2.2 Composition

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.2.3 Access to information and documents

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.2.3 Reporting to parliament

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.3 Expert oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The Irish experience of data retention oversight by a designated judge provides a good example of the limitations of non-specialist judicial oversight and the need for technical expertise or data protection authority input. I have summarised this in T.J. McIntyre, "Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective," in *Judges as Guardians of Constitutionalism and Human Rights*, ed. Martin Scheinin, Helle Krunke, and Marina Aksenova (Cheltenham: Edward Elgar, 2016) as follows:

> "Recently, however, two developments have exposed significant failings [in the effectiveness of the designated judge system]. In 2010 newspaper reports revealed that a detective sergeant abused the data retention system to spy on her ex-boyfriend.[59] This came to light due to his becoming suspicious – not due to any internal safeguards – and indicated a very serious flaw in the system, given that she was not authorised to make such requests. Remarkably, the only response of the designated judge in the next annual report was to say that "I am satisfied that the full extent of the alleged non-compliance with the Act has been rigorously investigated and fully understood and all appropriate steps taken to ensure future compliance". No account was given as to how the sergeant was able to circumvent the requirement of authorisation by a Chief Superintendent, or whether a Chief Superintendent might have been at fault in approving a request from her without due diligence. It should be noted that the incident also highlights failings in Garda discipline: the sergeant was not prosecuted for this offence, and instead was transferred to another sensitive role in the Special Branch.[60]
>
> Further concerns were raised in 2014 when the Data Protection Commissioner (DPC) published an audit into the handling of information in the Garda.[61] That audit identified a number of problems in relation to data retention, all of which the Designated Judge had failed to identify. Most fundamentally, the DPC found that there was a systematic practice of retrospectively rubberstamping requests whereby a "request is made without the Chief Superintendent's knowledge and signed/authorised retrospectively by the Chief Superintendent".[62] This practice essentially negated the statutory requirement that a request should only be made following consideration by a senior garda. The failure of the designated judge to identify such a deliberate and well established breach of the legislation – particularly after the 2010 incident – undermines any confidence in the oversight system.[63]
>
> It should be said, however, that these failings are only partly the result of the legislation itself – the statutory powers are wide enough that many of these points could be addressed if the designated judge and Complaints Referee took a more expansive approach. There is a very similar designated judge provision under the Criminal Justice (Surveillance) Act 2009, which regulates the use of surveillance devices such as covert video cameras and GPS. The statutory language is almost identical in setting out the oversight functions.[64] Despite this, the designated judges under the 2009 Act have made significantly greater use of their powers. Their annual reports are considerably more

[59] Nolan, L, 'Garda Detective Quizzed for 'Spying on Her Ex,'' *The Mail on Sunday*, June 27, 2010; Tighe, M., 'Garda Accused of Bugging Her Ex-Boyfriend,' *The Sunday Times*, February 20, 2011.
[60] Mooney, J., 'Garda Who Spied on Her Boyfriend Will Keep Job,' *The Sunday Times*, August 14, 2011, available at: http://www.thesundaytimes.co.uk/sto/news/ireland/News/Irish_News/article701376.ece.
[61] Data Protection Commissioner, 'An Garda Síochána: Final Report of Audit.'
[62] *Idem*, 64.
[63] The designated judge also failed to identify that requests were being made to companies who were not within the scope of the legislation: *Idem*, 63.
[64] Section 12, Criminal Justice (Surveillance) Act 2009.

15

detailed, generally running to 17 to 30 pages, including statistics as to the number of cases where surveillance has been used and a general assessment of its use.[65] They have also taken an active role in carrying out reviews – choosing a random selection of files, assessing the merits of the decision to use surveillance in each case and in some cases reviewing the surveillance evidence itself.

This difference in approach illustrates an important point: it is not enough to provide for judicial involvement in oversight without providing a clear model for what that oversight is expected to achieve and how it is to be achieved. Irish law has, in effect, asked the designated judges to craft their own role with varying degrees of success…

[W]e have also seen from the Irish experience that effective judicial oversight requires more than just judicial involvement – it requires thought as to what that involvement seeks to achieve, what resources are available and whether a particular function is best assigned to a judge. It is significant but not surprising that the audit by the Data Protection Commissioner identified issues which the designated judge did not. A generalist judge cannot be expected to have the specialist knowledge necessary to assess surveillance systems without either training or technical advisors."

I have attached a full copy of that chapter for your reference.

2.3.1 Specialised expert bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.3.2 Data protection authorities

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No suggestions for amendment of the text at section 2.3.2 of the Report. The text already captures the point that the Irish DPC may, in effect, examine national security issues only with the acquiescence of the Executive.

2.4 Approval and review of surveillance measures

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

[65] These annual reports are available at Digital Rights Ireland, 'Surveillance Library.'

16

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3 Remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3.1 A precondition: obligation to inform and the right to access

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

There is no provision in Irish legislation governing interception, data retention, surveillance devices or tracking devices which requires notification after the fact or permits an individual to access information as to whether they have been subject to surveillance.

The Criminal Justice (Surveillance) Act 2009 permits the Minister for Justice to make regulations which would provide for an individual to be notified that they had been subject to surveillance – however no such regulations have been made.[66]

Where an individual complains that they have been put under surveillance (in relation to data retention access, surveillance devices or interception of communications), the Complaints Referee is prohibited from confirming this to them unless he[67] finds that there has been a breach of the legislation in relation to the surveillance.[68] Even should the Complaints Referee find that there has been a breach, he has in some cases discretion to refuse to notify the individual of that fact if he considers "it would not be in the public interest to do so".[69] To date, there has never been a case in which the Complaints Referee has found a breach of the legislation.[70]

Data protection subject access requests to state bodies in relation to surveillance are also restricted. As already discussed, data protection law can be entirely excluded in the context of surveillance for state security purposes where so certified by the Minister for Justice or Minister

[66] Section 10(3).
[67] To date all the Complaints Referees have been men.
[68] See section 9(8) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 and section 11(7) of the Criminal Justice (Surveillance) Act 2009.
[69] Section 11(6) of the Criminal Justice (Surveillance) Act 2009.
[70] *Dáil Debates*, Written Answers, 4 March 2008.

17

for Defence. Even in a pure criminal justice context, the right of access is still excluded for personal data "kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders… in any case in which the application of [subject access requests] to the data would be likely to prejudice any of the matters aforesaid".[71]

Data protection subject access requests to private bodies may permit individuals to learn whether they have been the subject of surveillance in certain cases – typically where an individual asks a telecommunications company whether their mobile phone details have been accessed by any third party. However the practice of the Data Protection Commissioner has been inconsistent regarding such attempts to indirectly establish whether surveillance has been carried out.

In a 2002 case the Data Protection Commissioner adopted the same approach as the Complaints Referee, and adopted a practice of neither confirming nor denying that there had been police access to details of an individual's communications unless a telephone company had contravened the Data Protection Acts by providing access.[72]

However, in the 2014 DPC audit of An Garda Síochána the DPC took a different view, stating that where an individual makes a subject access request to a telecommunications company then details of any government requests for data should ordinarily be revealed as part of that request unless the investigating agency confirms that release would prejudice the investigation, prevention or detection of a crime.[73] In that audit the DPC statated that it intends to actively engage with the Garda Síochána to develop and issue sectoral advice in this regard. In an email of 18 July 2016 the DPC's Office stated that:

> "the DPC has not yet developed sectoral guidance but we intend to establish practice and review this area in Autumn 2016. At that time, we will conduct a series of audits of telcos which will examine this issue alongside a number of other areas requiring further examination on foot of findings from audits conducted by the Office Q1 and Q2 2016 of agencies prescribed under the Communications (Retention of Data) Act 2011 to make disclosure requests to telcos."

3.2 Judicial remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3.2.1 Lack of specialisation and procedural obstacles

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

[71] Section 5(1) of the Data Protection Acts 1988 and 2003.
[72] Data Protection Commissioner, 'Case Study 5/2002,' 2003, available at: https://www.dataprotection.ie/docs/Case-Study-5-02-Telephone-Company/114.htm.
[73] Data Protection Commissioner, 'An Garda Síochána: Final Report of Audit,' 65–66.

18

In Ireland the designated judge mechanism has been undermined by the fact that the role is a part-time one, carried out over a single day or a few days each year, where the designated judge does not have any special expertise in the area and does not have any technical or even administrative support for this function. This was highlighted in 2014 when a DPC audit of the handling of information in the Garda identified fundamental failings in the data retention system, which the designated judge had failed to identify.[74] The DPC found that there was a systemic practice of retrospectively rubberstamping requests whereby a "request is made without the Chief Superintendent's knowledge and signed/authorised retrospectively by the Chief Superintendent".[75] This breached the statutory requirement that a request should only be made following prior individual consideration by a senior garda. Similarly, the DPC identified that the legislation had been misapplied by the Garda Síochána, with requests for user information being made to firms which were not covered by the legislation.[76] Neither of these systemic problems had been identified by the designated judge in the 9 years since judicial oversight had been established.

Section 12(4) of the Communications (Retention of Data) Act 2011 permits the designated judge to communicate with the DPC in the exercise of his functions – presumably for assistance where necessary; however in an email of 18 July 2016 the Office of the DPC stated that there is: "no record of the Designated Judge having ever contacted the Office of the Data Protection Commissioner as per section 12(4) since the inception of the Act."

3.2.2 Specialised judges and quasi-judicial tribunals

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3.3 Non-judicial remedies: independence, mandate and powers

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3.3.1 Types of non-judicial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3.3.2 The issue of independence

[74] Data Protection Commissioner, 'An Garda Síochána: Final Report of Audit.'
[75] *Idem*, 64.
[76] Data Protection Commissioner, 'An Garda Síochána: Final Report of Audit,' 63.

19

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

3.3.3 Powers and specialisation of non-judicial remedial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Conclusions

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

1.5 Check the accuracy of the figures and tables published in the FRA report (see the annex on Figures and Tables)

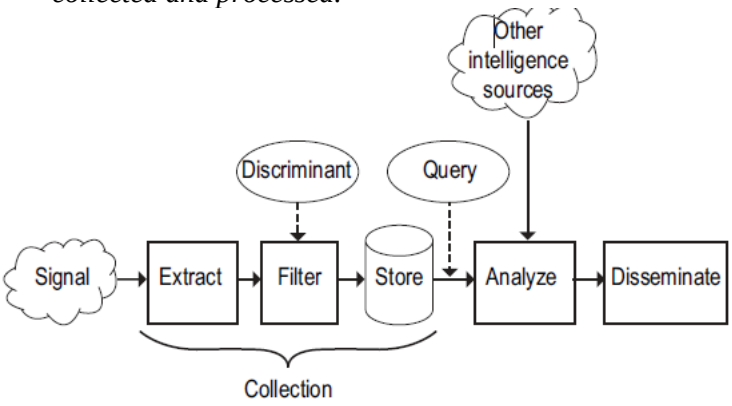
1.5.1 Overview of security and intelligence services in the EU-28

- *Please, delete all lines not referring to your country in the table below (see Annex p. 93 of the FRA Report)*
- *Check accuracy of the data*
- *Add in track changes any missing information (incl. translation and abbreviation in the original language).*
- *Provide the reference to the national legal framework when updating the table.*

	Civil (internal)	Civil (external)	Civil (i	Military
IE	The Crime and Security Branch within the Garda Síochána.Within the Crime and Security Branch, there is a specific Security and Intelligence section which is in turn divided into two subsections focusing on terrorism and organised crime respectively.[77]			Directorate of Intelligence (G2)

1.5.2 Figure 1: A conceptual model of signals intelligence

- *Please, provide a reference to any alternative figure to Figure 1 below (p. 16 of the FRA Report) available in your Member State describing the way signals intelligence is collected and processed.*



1.5.3 Figure 2: Intelligence services' accountability mechanisms

Please confirm that Figure 2 below (p. 31 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

[77] 'Crime & Security,' *An Garda Síochána - Ireland's National Police Service*, accessed April 27, 2016, available at: http://garda.ie/Controller.aspx?Page=40&Lang=1; Mulqueen, 'A Weak Link?,' 331–332.

21

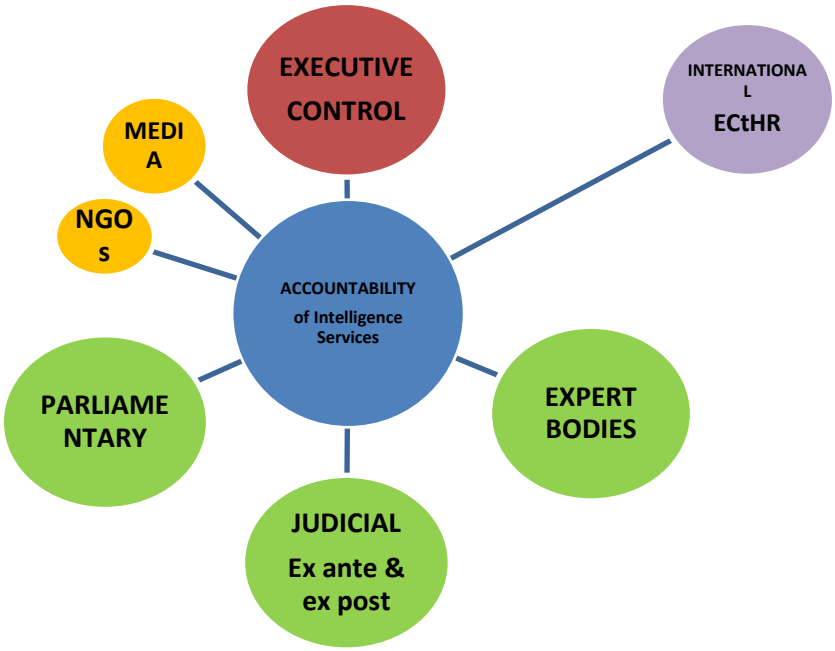

EXECUTIVE
CONTROL
INTERNATIONAL
ECtHR
MEDIA
NGOS
ACCOUNTABILITY
of Intelligence
Services
PARLIAMENTARY
EXPERT
BODIES
JUDICIAL
Ex ante &
ex post

Figure 2 would not be accurate in an Irish context. As already discussed there is no parliamentary or expert body oversight of the intelligence function within Ireland.

1.5.4 Figure 3: Forms of control over the intelligence services by the executive across the EU-28

Please confirm that Figure 3 below (p. 33 of the FRA Report) properly captures the executive control over the intelligence services in your Member State. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 3 does not capture the Irish context well. Specifically:

- The heads of the intelligence services are in effect the head of the police force (the Garda Commissioner) and the head of the Defence Forces (the Chief of Staff). In each case these are appointed by the Government acting as a whole, rather than by the Taoiseach or individual ministers.[78]
- The role of the Taoiseach (Prime Minister) is limited to appointing the Complaints Referee.[79]
- The other main oversight figures – the designated judges – are nominated by the President of the High Court following consultation with the Minister for Justice.[80]
- Because there is no distinct intelligence agency, the functions of issuing instructions, defining priorities, tasking, and approving surveillance are split between the Minister for Defence and Minister for Justice, depending on whether the surveillance is being carried out by the military or police forces.

1.5.5 Table 1: Categories of powers exercised by the parliamentary committees as established by law

Please, delete all lines not referring to your country in the table below (see p. 36 of the FRA Report)
Please check the accuracy of the data.. Please confirm that the parliamentary committee in your Member State was properly categorised by enumerating the powers it has as listed on p. 35 of the FRA Report. Please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Member States	Essential powers	Enhanced powers
IE		

Note: Finland, Ireland, Malta and Portugal do not have parliamentary committees that deal with intelligence services.

1.5.6 Table 2: Expert bodies in charge of overseeing surveillance, EU-28

Please, delete all lines not referring to your country in the table below (p. 42 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

[78] Section 12 of the Defence Act 1954; section 9 of the Garda Síochána Act 2005.
[79] Section 9 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.
[80] Section 8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993; section 12 of the Criminal Justice (Surveillance) Act 2009.

23

EU Member State	Expert Bodies
IE	Complaints Referee Designated Judges of the High Court

It must be noted that there are two separate designated judges – one appointed in respect of interception of communications and data retention[81], and the other appointed in respect of surveillance under the Criminal Justice (Surveillance) Act 2009 (covering, for example, the planting of bugs in buildings and the use of GPS tracking devices). This division of responsibilities is arguably undesirable as it means that there is no one judge with an overview of wider surveillance practices. It should also be mentioned that Irish legislation ties data retention and interception oversight together in the same designated judge, meaning that it would be misleading to discuss one without mentioning the other.

1.5.7 Table 3: DPAs' powers over national intelligence services, EU-28

Please, delete all lines not referring to your country in the table below (p. 49 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	No powers	Same powers (as over other data controllers)	Limited powers
IE			X

Notes: No powers: refers to DPAs that have no competence to supervise NIS.

Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.

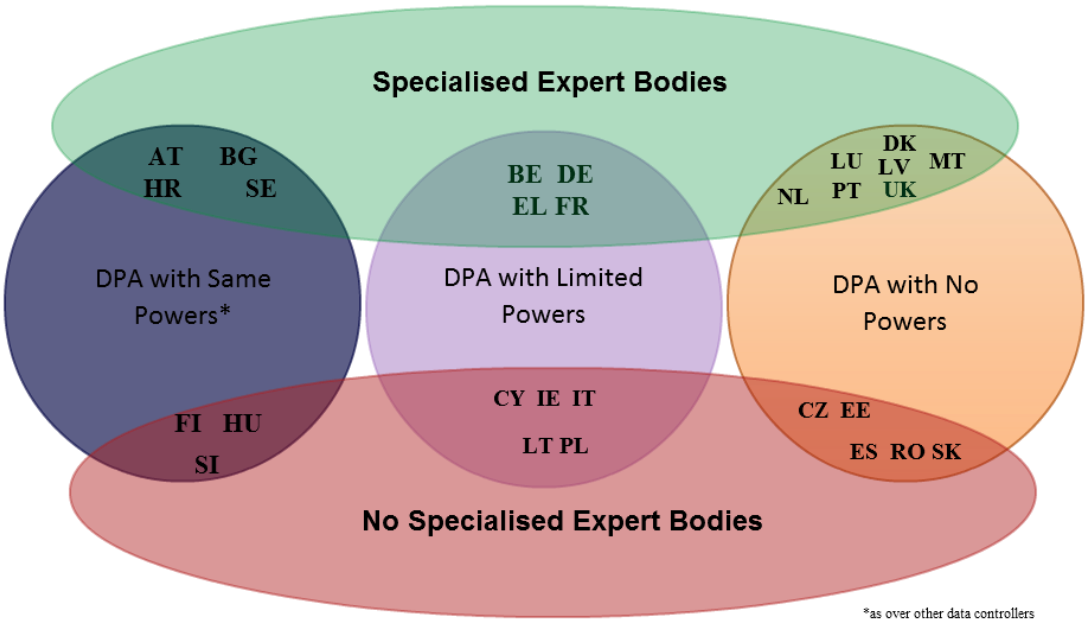
Limited powers: refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers) or to additional formal requirements for exercising them.

1.5.8 Figure 4: Specialised expert bodies and DPAs across the EU-28

Please check the accuracy of Figure 4 below (p. 50 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

[81] Under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 and Communications (Retention of Data) Act 2011.

24



1.5.9 Table 4: Prior approval of targeted surveillance measures, EU-28

Please, delete all lines not referring to your country in the table below (p. 52 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	Judicial	Parliamentary	Executive	Expert bodies	None
IE	X		X		

In Ireland prior judicial approval of targeted surveillance is only required in relation to "surveillance devices" (generally covert audio bugs or covert video cameras), where the Criminal Justice (Surveillance) Act 2009 requires prior judicial approval from the District Court, except in cases of urgency. It is correct to say that the other forms of targeted surveillance (in particular, planting of GPS tracker devices and interception of communications) require executive approval only.

1.5.10 Table 5: Approval of signals intelligence in France, Germany, the Netherlands, Sweden and the United Kingdom

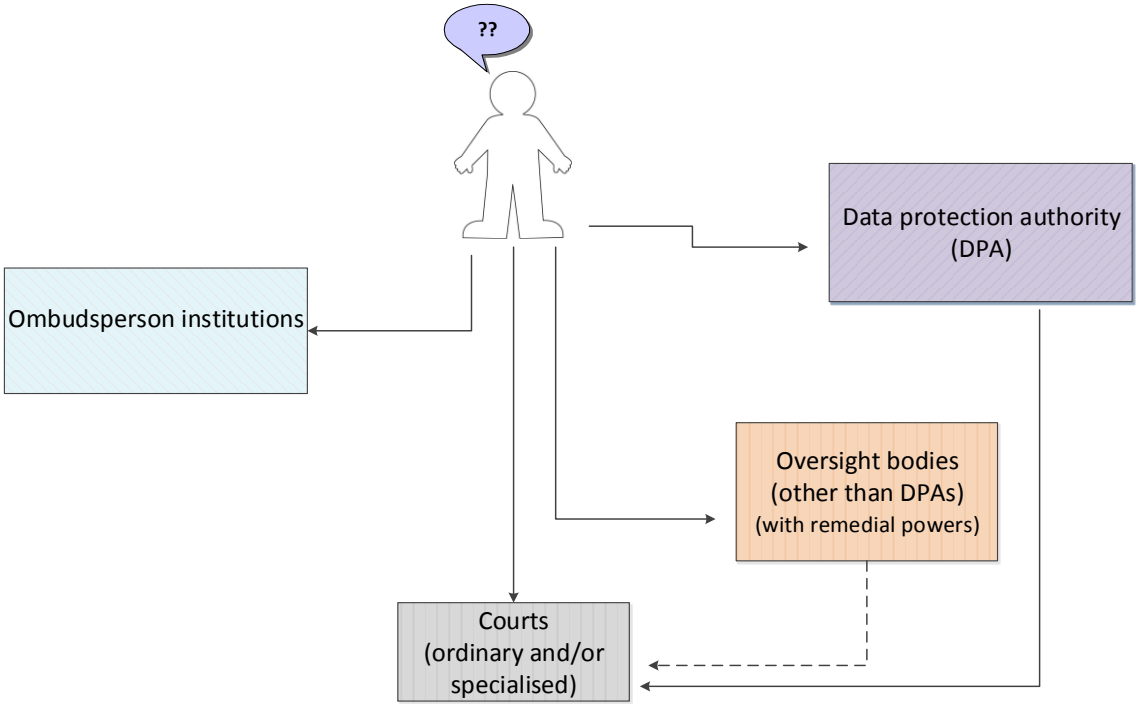
Please check the accuracy of Table 5 below (p. 55 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	Judicial	Parliamentary	Executive	Expert
FR			X	

DE		X (telco relations)		X (selectors)
NL			X (selectors)	
SE				X
UK			X	

1.5.11 Figure 5: Remedial avenues at the national level

Please confirm that Figure 5 below (p. 60 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



As already discussed in section 1.2, in an Irish context the Data Protection Commissioner has relatively limited power to investigate complaints of surveillance relating to an intelligence and state security function, insofar as both the Minister for Justice and Minister for Defence can disapply data protection law in relation to particular information by confirming that such information is held for the purposes of state security.

In relation to the Garda Síochána, there is an ombudsman function carried out by the Garda Síochána Ombudsman Commission (GSOC). The role of GSOC has already been discussed in section 1.2 above, where we noted that it does not appear to have power to review surveillance or intelligence sharing functions unless these amount to either criminal offences or breaches of discipline:

> "This body has the power to investigate complaints regarding allegations of misbehaviour by a member of the Garda Síochána, meaning conduct which "constitutes an offence or a breach of discipline".[82] This power could, in principle, be used to investigate complaints of illegal surveillance by a member but would not permit an

[82] Sections 82 and 87 of the Garda Síochána Act 2005.

26

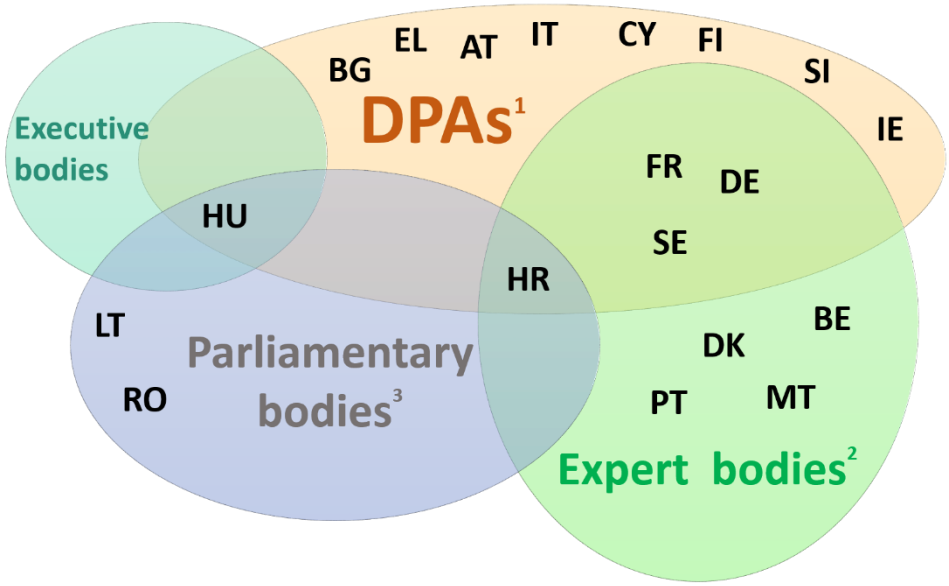
investigation of wider surveillance and intelligence sharing practices unless these constituted criminal offences or breaches of discipline. Since 2015 GSOC has has the power to carry out wider investigations of Garda "practices, policies and procedures", but only insofar as this is for the purpose of preventing or reducing complaints.[83] For that reason, this power would not appear to permit GSOC to investigate surveillance and intelligence practices."

While there is also a general Ombudsman with a remit in respect of the wider public sector, that official does not have any power to review the actions of "exempt bodies". These include the two bodies with an intelligence and state security function – i.e. the Defence Forces and the Garda Siochana – which are therefore entirely outside the remit of the Ombudsman.[84]

Apart from these points, this diagram would be accurate for Ireland.

1.5.12 Figure 6: Types of national oversight bodies with powers to hear individual complaints in the context of surveillance, by EU Member States

Please check the accuracy of Figure 6 (p. 73 of the FRA Report) below. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



Notes: 1. The following should be noted regarding national data protection authorities: In Germany, the DPA may issue binding decisions only in cases that do not fall within the competence of the G 10 Commission. As for 'open-sky data', its competence in general, including its remedial power, is the subject of on-going discussions, including those of the NSA Committee of Inquiry of the German Federal Parliament

[83] Section 10 of the Garda Síochána Amendment Act 2015, substituting section 106 of the Garda Síochána Act 2005.
[84] Ombudsman (Amendment) Act 2012, Schedule Part 2. In addition, section 5(1)(b) of the Ombudsman Act 1980 prevents the Ombudsman from investigating any action which 'relates to or affects national security or military activity'.

27

2. *The following should be noted regarding national expert oversight bodies: In Croatia and Portugal, the expert bodies have the power to review individual complaints, but do not issue binding decisions. In France, the National Commission of Control of the Intelligence Techniques (CNCTR) also only adopts non-binding opinions. However, the CNCTR can bring the case to the Council of State upon a refusal to follow its opinion. In Belgium, there are two expert bodies, but only Standing Committee I can review individual complaints and issue non-binding decisions. In Malta, the Commissioner for the Security Services is appointed by, and accountable only to, the prime minister. Its decisions cannot be appealed. In Sweden, seven members of the Swedish Defence Intelligence Commission are appointed by the government, and its chair and vice chair must be or have been judges. The remaining members are nominated by parliament.*
3. *The following should be noted regarding national parliamentary oversight bodies: only the decisions of the parliamentary body in Romania are of a binding nature.*

Insofar as the Irish DPC has a possible, though limited, role in investigating complaints and the Complaints Referee would appear to be an "expert body" for the purposes of Figure 6, then perhaps Ireland should appear next to FR, DE and SE in the diagram? That said, it is not clear to me from the 2015 report whether the Complaints Referee should properly be considered to be an "expert body" – as noted earlier, the role is carried out on a part time basis by an individual judge who is not required to have any special expertise in the area and who is not assisted by any technical advisers. If this does not meet the FRA criteria for an "expert body" then Ireland should properly remain where it is on the diagram.