PRIVACY INTERNATIONAL

Stakeholder Report Universal Periodic Review
Submission: 25th Session

The Right to Privacy in Ireland

Submitted by
Privacy International and Digital Rights Ireland
September 2015

PRIVACY INTERNATIONAL

Digital Rights Ireland

I. Introduction

1. This stakeholder report is a submission by Privacy International (PI) and Digital Rights Ireland Ltd. (DRI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. DRI is an Irish group dedicated to defending civil, legal and human rights in a digital age.[1]

2. PI and DRI wish to bring concerns about the protection and promotion of the right to privacy in Ireland before the Human Rights Council for consideration in Ireland's upcoming review.

II. The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[2] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

4. Activities that restrict the right to privacy, such as surveillance, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[4] A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law.[6]

III. Follow up to the previous UPR

6. There was no mention of the right to privacy in the National Report submitted by Ireland in 2010, nor in the stakeholder submissions and the issue was not addressed in the report of the Working Group following the consideration of the state report in 2011. Because of this lack of scrutiny it is particularly appropriate to raise the issue

1 This submission has been prepared by Dr. TJ McIntyre (DRI) and Ms. Alexandrine Pirlot de Corbion (PI).
2 Universal Declaration of Human Rights (Article 12), International Covenant on Civil and Political Rights (Article 17); regional treaties and standards including the African Charter on the Rights and Welfare of the Child (Article 10), the American Convention on Human Rights (Article 11), the African Union Principles on Freedom of Expression (Article 4), the American Declaration of the Rights and Duties of Man (Article 5), the Arab Charter on Human Rights (Article 21), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8).
3 See Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014.
4 Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).
5 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)
6 As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (December 8, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

now in light of recent developments which have identified problems with Irish law in relation to regulation of state surveillance.

IV. Domestic laws related to privacy

7. The Constitution of Ireland does not explicitly guarantee a right to privacy but the courts have recognised an unenumerated right to privacy as one of the personal rights in the Constitution.[7]

8. Irish law provides a statutory right to data protection in the Data Protection Acts 1988 and 2003, implementing the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[8] and EU Data Protection Directive 95/46/EC.

9. The ePrivacy Regulations 2011[9] address data protection for phone, e-mail and Internet use, and give effect to the EU ePrivacy Directive 2002/58/EC.[10]

10. The European Convention on Human Rights has been brought into force in Ireland with the adoption of the European Convention on Human Rights Act 2003. That Act gives effect to Article 8 of the European Convention on Human Rights which provides:

> "*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

V. International obligations

11. Ireland is a signatory to the Universal Declaration of Human Rights ('UDHR') and has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "*no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*". The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "*adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy].*"[11]

12. Ireland is a party to the European Convention on Human Rights, which, as has already been noted, has been incorporated into domestic law. In matters within the scope of European Law, Ireland is bound by the Charter of Fundamental Rights of the European Union, Articles 7 and 8 of which relate to the right to privacy and the protection of personal data respectively.

7 McGee v. Attorney General [1974] IR 284; Kennedy and Arnold v. Attorney General [1987] IR 587.
8 ETS No. 108.
9 S.I. 335 of 2011.
10 As amended by Directive 2006/24/EC and 2009/136/EC)
11 General Comment No. 16 (1988), para. 1

13. Ireland has ratified the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[12]

VI. Areas of concern

No general requirement for prior judicial authorisation of state surveillance

14. Broadly speaking, Irish law regulates four types of state surveillance:

    - Interception of communications under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 (the "1993 Act")[13]
    - Access to retained communications data (data retention) under the Communications (Retention of Data) Act 2011 (the "2011 Act")
    - The use of "tracking devices" (such as GPS trackers placed on cars or other vehicles) under section 8 of the Criminal Justice Surveillance Act 2009 (the "2009 Act")[14], and
    - The use of "surveillance devices" (such as audio bugs and covert video cameras) under section 7 of the 2009 Act.

15. Of these forms of surveillance, only the last – the use of "surveillance devices" in a narrowly defined sense[15]– requires prior judicial authorisation.[16] The interception of communications requires only the authorisation of the Minister for Justice and Equality[17] while the use of tracking devices[18] and access to retained communications data take place solely on the basis of internal approval within the Garda Síochána (police force), Permanent Defence Force (military) or the Revenue Commissioners (tax authorities).[19]

16. Systems of internal approval are particularly open to abuse, and in 2010 a sergeant in the Garda Síochána was discovered to be using the data retention system to spy on her former partner.[20] It appears this emerged due to his suspicions and not due to any internal controls.[21] Despite this, the sergeant in question was not prosecuted, dismissed, nor demoted, and she was transferred to a sensitive position in the Special Branch (anti-terrorist division). No details have been published as to how she was able to avoid the controls which should have prevented her abusing her access in this way, nor has the Irish State detailed any steps to review the operation of the data retention system in light of this incident.

Judicial authorisation under the Criminal Justice (Surveillance Act) 2009 can be bypassed.

17. The 2009 Act was a positive development in Irish law for the way in which it introduced a requirement of prior judicial authorisation before the use of certain "surveillance devices". This term is defined in section 1 and will, for example, include audio bugs and video cameras covertly planted in properties.

12 ETS No. 108.
13 See Maurice Collins, "Telephone Tapping and the Law in Ireland," Irish Criminal Law Journal 3 (1993): 31.
14 See Alisdair A. Gillespie, "Covert Surveillance, Human Rights and the Law," Irish Criminal Law Journal 19, no. 3 (2009): 71.
15 As defined in section 1 of the Criminal Justice Surveillance Act 2009.
16 Section 5 of the Criminal Justice (Surveillance) Act 2009.
17 Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.
18 Section 8 of the Criminal Justice (Surveillance) Act 2009.
19 Section 6 of the Communications (Retention of Data) Act 2011.
20 Mooney, "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.
21 Larissa Nolan, "Garda Detective Quizzed for 'Spying on Her Ex,'" The Mail on Sunday, June 27, 2010; Mark Tighe, "Garda Accused of Bugging Her Ex-Boyfriend," The Sunday Times, February 20, 2011.

18. However, this judicial authorisation can be entirely bypassed under Section 7 of the 2009 Act, which provides that a superior officer within the Garda Síochána, Permanent Defence Force or Revenue Commissioners can provide internal approval in cases of urgency – allowing this type of surveillance to take place for up to 72 hours without any judicial authorisation either before or after the fact. This provision was heavily criticised at the time of the enactment of the legislation and could have been avoided by ensuring that a judge is available by telephone to authorise urgent requests as and when needed.[22] It is also of questionable constitutionality in that it purports to permit a secret invasion of the dwelling house (to plant and remove bugs) without prior judicial approval – contrary to Irish law which generally requires a judicial warrant before searches of the home.[23]

No statutory controls on use of informants or undercover police

19. Another significant form of surveillance is the use of informants and undercover police. This has been acknowledged in other jurisdictions – such as the United Kingdom – as giving rise to particular fundamental rights issues due to its intrusion into private lives as well as the potential for abuse.[24] In an Irish context the issue of informants has been controversial for many years and has led to a Government appointed Tribunal of Inquiry finding that the use of informants had been poorly managed to the point of being "chaotic".[25] Despite this, there is no legislation in Ireland regulating the use of either informants or undercover police.[26]

No notification of surveillance after the fact

20. Notification of individuals who have been the subject of surveillance measures has been recognised by the European Court of Human Rights as an important safeguard for the right to privacy, serving both to deter improper surveillance and to provide individuals with an effective remedy before the courts in the case of abuse.[27] Irish law does not, however, require such notification.

21. In the case of interception of communications and data retention, neither the 1993 Act nor the 2011 Act require – or even permit – the notification of individuals that they have been the subject of surveillance. Indeed the 1993 Act appears to rule out any such notification – even in cases where it is determined that an interception of communications should not have taken place – by imposing secrecy obligations in relation to the fact of interceptions.[28]

22. The position should be different under the 2009 Act. That Act provides that the Minister for Justice and Equality may make regulations for the disclosure of

22 Gillespie, "Covert Surveillance, Human Rights and the Law."
23 Compare Damache v DPP [2012] IESC 11.
24 See e.g. Roger Billingsley, Covert Human Intelligence Sources: The "Unlovely" Face of Police Work (Waterside Press, 2009).
25 See e.g. Fitzgerald, "The Morris Tribunal and the Garda Síochána," Garda Communique, March 2008, http://www.garda.ie/Documents/User/communique%20mar%2008.pdf; Irish Council for Civil Liberties, Implementing Morris: An Agenda for Change (Dublin: 2006), pp.18-20.
26 As regards informants, since 2006 there has been an internal administrative code of practice within the Garda Síochána and since 2010 an ad hoc system of oversight by a retired judge. See Liz Campbell, "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; T.C. Smyth, "Covert Human Intelligence Sources: Report of Independent Oversight Authority," October 2, 2012,. Available at: https://www.digitalrights.ie/dri/wp-content/uploads/2014/07/CHIS-2012.pdf; Dermot Walsh, Human Rights and Policing in Ireland: Law, Policy and Practice (Dublin: Clarus Press, 2009), chap. 27.
27 See e.g. Franziska Boehm and Paul De Hert, "Notification, an Important Safeguard against the Improper Use of Surveillance – Finally Recognized in Case Law and EU Law," European Journal of Law and Technology 3, no. 3 (2012). Available at: http://ejlt.org/article/view/155.
28 Sections 10 and 12.

information about the use of a tracking or surveillance device to the person who was placed under surveillance or other persons who were materially affected by the surveillance.[29] This provision was introduced by the Minister on the basis that it "*takes account of European Court of Human Rights jurisprudence, which has found that a provision allowing disclosure in at least certain circumstances is required and that it is an important safeguard where an improper use of surveillance might occur.*"[30]

23. However, despite the Minister describing this as "required" under the ECHR and "an important safeguard", no such regulations have been made. This effectively negates the statutory provision for notification under the 2009 Act and ensures that there is no notification obligation or even discretion in respect of any form of state surveillance in Ireland.

Oversight of state surveillance

Inadequate oversight of interception and data retention

24. Irish law does not provide for any oversight of state surveillance by parliament or any independent statutory body. Instead, the 1993 Act established a judicial oversight system for the interception of communications which has been extended to cover data retention under the 2011 Act also. This system has two distinct judicial roles.

Designated Judge

25. For general oversight a "designated judge" – a High Court judge, nominated by the President of the High Court – is given the functions of keeping the operation of the legislation under review, ascertaining whether the authorities are complying with its provisions and providing an annual report to the Taoiseach (Prime Minister) including such matters as he thinks appropriate.[31]

26. However this system has proven inadequate.[32] Since the creation of the role, the annual reports have consisted exclusively of a few formulaic paragraphs which recite that on a particular day certain (unspecified) documents were inspected, certain (unspecified) queries answered and as a result the judge is satisfied that the relevant authorities are in compliance with the law.[33]

27. These reports provide no indication as to the methodology used (are random disclosure requests chosen and audited; are internal systems reviewed?), no statistics as the number of interceptions which are being carried out, no indication of the circumstances in which these powers are being used, and no indication of the safeguards (if any) in place to prevent abuse or rectify errors.

28. The reports also reflect a wider problem - the oversight role is an ad hoc, after the fact, part-time function of a busy judge with no staff, specialist training or technical

29 Section 10(3).
30 Dáil Debates, Thursday 25 June 2009, available at http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/dail2009062500005?opendocument
31 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.
32 Cormac O'Keeffe, "More Robust Oversight of Surveillance Laws Is 'Crucial', Experts Warn," Irish Examiner, June 15, 2015,. Available at: http://www.irishexaminer.com/ireland/more-robust-oversight-of-surveillance-laws-is-crucial-experts-warn-336910.html.
33 The annual reports of the designated judge and other official materials are available at Digital Rights Ireland, "Surveillance Library," accessed March 25, 2015. Available at: https://www.digitalrights.ie/irish-surveillance-documents/.

The most recent report, reproduced below in full, is typical:

Report of the Designated Judge Pursuant to Section 8(2) of the Interception of Postal Packets and Telecommunication Messages (Regulation) Act 1993 and Section 12(1)(c) of the Communications (Retention of Data) Act 2011

I am the "Designated Judge" under the above mentioned Acts.

On 24th October, 2014, I attended at the Headquarters of An Garda Síochána at "the Depot", Phoenix Park, Dublin and later in the afternoon of the same day, at the Headquarters of the Army in McKee Barracks, Blackhorse Avenue, Dublin.

On 31st October, 2013, I attended at the Office of An Garda Síochána Ombudsman Commission, 150 Upper Abbey Street, Dublin and later on the afternoon of the same date at the Office of the Revenue Commissioners, Block D, Ashtown Gate, Dublin 15.

On the morning of 6th November, 2014, I attended at the Office of the Department of Justice and Equality, St. Stephen's Green, Dublin 2.

In each of these locations, such documents and records pertaining to the operation of the above Acts as were requested by me, were made available and were examined by me. I also spoke with the persons with responsibility for and overseeing the operation of the above Acts, in each location and all of my queries were answered to my satisfaction.

I am satisfied that as of the date of this report, the relevant State authorities are in compliance with the provisions of the above Acts.

Mr. Justice Paul McDermott
13th November, 2014

advisors. It is therefore prone to over-reliance on the entities supposedly being monitored.[34]

29. This has been highlighted by two recent examples of abuse, neither of which were identified by the Designated Judge. We have already mentioned a 2010 case in which a Garda sergeant was found to be using the data retention system to spy on her former partner.[35] 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 for internal authorisation, or whether a superior been had been at fault in approving a request from her without due diligence.

30. A further issue emerged in 2014 when the Data Protection Commissioner (DPC) published an audit into the handling of information in the Garda Síochána.[36] 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 rubber stamping requests whereby a "*request is made without the Chief Superintendent's knowledge and signed/ authorised retrospectively by the Chief Superintendent*".[37] This practice negated the statutory requirement that a request should only be made following prior authorisation by a senior officer. 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.[38]

Complaints Referee

31. A redress mechanism involves a "Complaints Referee" who is appointed by the Taoiseach for a five year term and in practice is always a Circuit Court judge.[39] The Complaints Referee can investigate complaints that communications have been intercepted or data relating to a person has been accessed following a disclosure request, and if they find that certain breaches of the 1993 Act or 2011 Act have taken place they shall notify the complainant of their finding and make a report to the Taoiseach. They may also order that the relevant data be destroyed and that compensation be paid. The Complaints Referee has powers to access and inspect any official records and to request any information relating to an interception or data disclosure request.

32. This complaints investigation system is, in principle, desirable. However a lack of transparency makes it impossible to determine its effectiveness in practice. The investigations and decisions of the Complaints Referee are not published and the Irish Government has stated that it does not hold records on the number of complaints

34 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, forthcoming).
35 Mooney, "Garda Who Spied on Her Boyfriend Will Keep Job."
36 Data Protection Commissioner, "An Garda Síochána: Final Report of Audit," March 2014. Available at: http://www.garda.ie/Documents/User/An%20Garda%20S%C3%ADoch%C3%A1na%20ODPC%20Report%20Final.pdf.
37 Ibid., 64.
38 The designated judge also failed to identify that requests were being made to companies who were not within the scope of the legislation: Ibid., 63.
39 Section 9, Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

received or any details of such complaints.[40] However, it appears that there has never been a successful complaint to the Complaints Referee in respect of either wrongful interception of communications or wrongful access to communications data.[41]

Failure to provide statistics

33. The Irish Government does not provide statistics on the number of cases in which communications are intercepted and has prevented communications providers from reporting this information, despite not having any legal basis for doing so. In 2014, Vodafone published a Transparency Report in which it stated that it "cannot disclose" the number of interception requests it received, stating that "*Whilst local laws do not expressly prohibit disclosure, we asked the authorities for guidance and have been informed that we cannot disclose this information*".[42] When Vodafone updated their report in February 2015, they noted that "*During 2014-15, we engaged extensively with the government to discuss whether or not such information could be published by the authorities themselves or – if not – by Vodafone and other operators. The government has again informed us that we cannot disclose this information.*"[43]

Oversight of tracking devices and surveillance devices

34. The Criminal Justice (Surveillance) Act 2009 has copied the Designated Judge / Complaints Referee system to provide oversight in relation to the use of tracking devices and surveillance devices. However the Designated Judge role under the 2009 Act is a separate one which is held by a different judge of the High Court.

35. While the statutory language under the 2009 Act is almost identical to that of the 1993 and 2011 Acts, the two judges who have held the role of Designated Judge under the 2009 Act have made significantly greater use of their powers.[44] Their annual reports have been considerably more detailed, generally running to 17 to 30 pages, and have included statistics as to the number of cases where surveillance has been used and a general assessment of its use.[45] 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.

36. These judges have demonstrated that it is possible to provide significantly greater transparency and statistics around the operation of state surveillance, without jeopardising any national security interest, and the approach which they have taken under the 2009 Act should be followed in relation to the interception of communications and access to communications data also.

Inadequacies in interception of communications law

37. The interception of telecommunications in Ireland is regulated by the Postal and

40 Dan MacGuill, "State Surveillance: How Gardaí and Others Can Secretly Monitor You," TheJournal.ie, May 17, 2015. Available at: http://www.thejournal.ie/state-surveillance-ireland-gardai-wiretapping-email-monitoring-gardai-2099537-May2015/.
41 Dáil Debates, Written Answers, 4 March 2008, 122-123. Available at: http://debates.oireachtas.ie/dail/2008/03/04/unrevised2.pdf
42 Jack Horgan-Jones, "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/.
43 See: Vodafone, Country -by-country disclosure of law enforcement assistance demands, 2015. Available at: http://www.vodafone.com/content/index/about/sustainability/law_enforcement/country_by_country.html
44 See section 12, Criminal Justice (Surveillance) Act 2009.
45 These annual reports are available at Digital Rights Ireland, "Surveillance Library."

Telecommunications Services Act 1983 (the "1983 Act") as amended by the 1993 Act. These laws predate the modern internet, and this is reflected in significant gaps when applying them to modern technology.

No regulation of interception of internet communications services

38. The 1983 and 1993 Acts are limited in their scope and do not protect many forms of internet communications services. The offence of interception of communications as originally enacted in 1983 applied only to messages being transmitted by the state monopoly provider Telecom Éireann.[46] With the progressive liberalisation of the telecoms market it was extended in 1999[47] to messages being transmitted by "licensed operators" and in 2003 to messages being transmitted by "authorised undertakings".[48] These terms, broadly speaking, cover landline, cable and mobile phone providers, and fixed and mobile internet service providers. They do not, however, include services such as Gmail, Hotmail, WhatsApp, Facetime, iMessage, Snapchat, Viber, etc. as the providers of these services will not be "licensed operators" or "authorised undertakings" for the purposes of Irish telecoms law.[49]

39. The significance of this point is that there is no offence in Irish law which criminalises surveillance of these types of communication. If, for example, an employee of Viber were to read user messages as they were transmitted through Viber's servers then no interception offence would be committed as the messages would not, at that point, meet the statutory requirement of "being transmitted" by a "licensed operator" or "authorised undertaking".[50]

40. A knock on effect is that there is no statutory regulation of the manner in which the Irish state may carry out surveillance against these services. The provisions of the 1983 and 1993 Acts – such as the principle of Ministerial approval of interceptions, the role of the Designated Judge and the role of the Complaints Referee – apply only to "interceptions" as defined by the 1983 Act. Surveillance of services such as Viber would, as we have seen, fall outside that definition and therefore would not be regulated by the 1983 and 1993 Acts. Consequently it is unclear what protections, if any, are in place for users of these services against either state or criminal interception of their messages.

No protection for stored communications

41. There is no explicit protection in Irish law for communications messages which are no longer in transit but are stored by a third party (as in the case of webmail).

42. Stored communications are particularly sensitive. While real-time interception of communications exposes a person's private life at a particular point in time, access to all their previous stored communications – often going back many years – will provide a record of their entire life over that period and is therefore significantly more invasive. This has been acknowledged by e.g. the United States Stored Communications Act which provides for additional protections before access to the content of messages stored by internet firms.[51]

46 Section 98 of the 1983 Act.
47 Section 7 of the Postal and Telecommunications Services (Amendment) Act, 1999.
48 European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2003 (S.I. 306 of 2003).
49 Denis Kelleher, Privacy and Data Protection Law in Ireland (Dublin: Tottel, 2006), 454. Section 98 of the 1983 Act.
50 Section 98 of the 1983 Act.
51 See e.g. Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," George Washington Law Review 72 (2004): 1208.

43. Despite this, state access to stored communications is not regulated by Irish interception laws. There are two reasons for this. First, as we have already seen, the most significant internet communications services – Gmail, Hotmail, etc. - fall outside the scope of the 1983 and 1993 Acts as they will not be "licensed operators" or "authorised undertakings" for the purposes of Irish telecoms law.[52] Second, the definition of "interception" in the 1983 and 1993 Acts is restricted to real-time interceptions. Section 98(1) of the 1983 Act, as amended, criminalises interception of messages "*being transmitted*" while section 98(6) goes on to define interception as to "*listen to, or record by any means, in the course of its transmission, a telecommunications message*". These references to a message "being transmitted" and "in the course of its transmission" make it clear that the legislation was not intended to apply to stored messages.

44. This lack of regulation has not, however, prevented the Irish authorities from accessing stored communications despite the absence of any specific authority to do so – for example, Microsoft Transparency reports have revealed numerous requests for access to the contents of webmail, a number of which have been granted.[53]

45. The Department of Justice and Equality has refused to specify the legal basis on which such requests are made.[54] However it appears that the usual practice is to request firms to make voluntary disclosure of stored communications, on the basis that data protection law permits such disclosure where it is "*required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders*".[55] There is no requirement for any form of external approval before this is done, no oversight of the process by an independent body, no notification of the user and no complaints mechanism for wrongful access to communications.

46. This practice – by acquiring the contents of communications without any clear legal basis, prior judicial approval, subsequent judicial oversight or redress mechanism – runs directly counter to the requirements of ECHR caselaw from Klass v. Germany onwards which requires that at a minimum there must be oversight mechanisms established by law which are "independent of the authorities carrying out the surveillance", "objective" and "vested with sufficient powers and competence to exercise an effective and continuous control" over the surveillance.[56]

Unclear whether Irish state can or does require direct access to telecommunication provider networks

47. Section 110 of the 1983 Act as amended provides that the Minister for Posts and Telegraphs (now the Minister for Communications, Energy and Natural Resources) may issue directions in writing to an "authorised undertaking" requiring them to do anything which the Minister may specify from time to time as necessary in the national interest. This statutory power is used to require interception in individual cases – but given the breadth of this section and the lack of controls on its use it appears that it could also be used to require telecommunications providers to build in backdoors

52 Kelleher, Privacy and Data Protection Law in Ireland, 454.
53 "Microsoft Law Enforcement Requests Report," accessed October 1, 2015. Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.
54 "Gardaí Sought Access to Hundreds of Private Emails," Irish Examiner, March 22, 2013. Available at: http://www.irishexaminer.com/ireland/gardai-sought-access-to-hundreds-of-private-emails-226189.html.
55 Section 8 of the Data Protection Acts 1988 and 2003. See in particular Annette Hogan, "The Interception of Communications in Ireland - Time for a Re-Think," Data Protection Ireland 7, no. 5 (2014): 9.
Communications in Ireland - Time for a Re-Think," Data Protection Ireland 7, no. 5 (2014): 9.
56 Klass v. Germany, application 5029/71, 6 September 1978, para. 56.

giving the Irish state direct access to their systems. According to Vodafone's 2014 Law Enforcement Disclosure Report: "*under section 110 of the 1983 Act, the Minister's powers seem sufficiently broad to allow implementation of a technical capacity that enables direct access to a Licenced Operator's network (without the Licenced Operator's operational control or oversight)*".[57]

48. Although Vodafone did not identify which countries do in fact demand direct access to its network, media reports since then have suggested that Ireland is one such country.[58] The significance of this point is that systems of direct access bypass safeguards around surveillance and make abuses more likely. Vodafone's group privacy officer summarised this at the time, stating that: "*Without an official warrant, there is no external visibility. If we receive a demand we can push back against the agency. The fact that a government has to issue a piece of paper is an important constraint on how powers are used*".[59]

49. Ministerial directions under section 110 are treated as secret (although there is no legal basis for this secrecy) and following an amendment of the law in 2008 prosecutions for failure to comply with a direction may be prosecuted in camera – that is, in complete secrecy with the public and the media being prevented from knowing about the fact of the prosecution.[60] This creates the possibility for companies to face secret prosecutions based on secret interpretations of secret ministerial directions – entirely ruling out any public scrutiny in this area and creating a significant risk of abuse.[61]

Continued use of data retention

50. Although the EU Data Retention directive was declared invalid by the Court of Justice of the European Union (CJEU) in April 2014 following the constitutional challenge brought by Digital Rights Ireland, the Irish state has failed to make any changes to the domestic data retention system which would address the grave concerns raised by the CJEU.[62]

51. The CJEU noted that metadata may allow "*very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained*" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[63] This point has been reinforced by a number of human rights experts including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[64]

57 Vodafone, Law Enforcement Disclosure Report, Legal Annex, February 2015, p. 43. Available at: https://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf

58 Pope, "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; Lillington, "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.

59 Garside, "Vodafone Reveals Existence of Secret Wires That Allow State Surveillance," The Guardian, June 6, 2014. Available at: http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance.

60 Section 30, Criminal Justice (Mutual Assistance) Act 2008.

61 Karlin Lillington, "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.

62 See Court of Justice of the European Union, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, judgment of 8 April 2014.

63 See Court of Justice of the European Union, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, judgment of 8 April 2014.

64 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

52. However, contrary to the requirements articulated by the CJEU under Articles 7 and 8 of the Charter of Fundamental Rights, Irish law continues to provide for a two year retention period for telephony data and one year for internet data, which is applied indiscriminately to all citizens without any element of prior suspicion and without any judicial or independent approval before such data can be accessed.

53. The case brought by Digital Rights Ireland continues before the Irish courts and seeks to invalidate the domestic law also.[65]

Inadequate protections against IMSI catchers

54. In February 2014, allegations were made regarding surveillance against the Garda Síochána Ombudsman Commission (GSOC). As a result of an investigation conducted by a UK-based counter-surveillance company, Verrimus, evidence emerged that an IMSI catcher device may have been deployed near the GSOC's offices.[66] An IMSI catcher is a phone monitoring kit that provides active intercept capabilities by presenting itself as the strongest base station to which phones connect which allows it to obtain IMEI and the IMSI: identifiers for your phone and SIM Card which are then used to monitor the operations of the phone.[67]

55. Following these revelations, the Minister for Justice and Equality, Alan Shatter, appeared before a parliamentary committee on 19 February 2014. The Minister made several worrying comments at that hearing – in particular, stating that IMSI catchers may be lawfully available to anyone, and given their low cost they are now accessible to everyone, and not just government agencies. In addition, he noted that the open access of the Ireland's current mobile phone infrastructure made all users "extraordinarily vulnerable" to interception of calls, texts and emails.[68]

56. IMSI Catchers allow attackers to indiscriminately gather data from thousands of mobile phones in a specific area and at public events such as political demonstrations. The lack of transparency around their use and the uncertainty as to the legal basis for their use in Ireland are highly concerning. It is not clear, based on the Minister's comments, whether the Irish state considers that the use of IMSI catchers constitutes an "interception" of communications regulated by the 1983 and 1993 Acts – if not, there is an urgent need for legislation criminalising their use.

Attempted purchase of surveillance malware without legal basis

57. In 2015 leaked emails from Italian-based spyware developer, Hacking Team, revealed that members of the Permanent Defence Force had been in discussion with Hacking Team to purchase their products.[69] Hacking Team sell a remote control system called Galileo which is a form of malware allowing purchasers to take control of a computer or phone to spy on users without their knowledge. Hacking Team sells this as a tool to "*bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain*".[70]

65 Noel Baker, "EU Court Rules Data Retention Directive Is Invalid," Irish Examiner, April 9, 2014. Available at: http://www.irishexaminer.com/ireland/eu-court-rules-data-retention-directive-is-invalid-264719.html.
66 Privacy International, "€5000 to compromise Ireland's mobile phone infrastructure", 27 February 2014. Available at: https://www.privacyinternational.org/?q=node/163
67 For further details, please see: Privacy International, Phone Monitoring, https://privacyinternational.org/?q=node/76
68 Privacy International, "€5000 to compromise Ireland's mobile phone infrastructure", 27 February 2014. Available at: https://www.privacyinternational.org/?q=node/163
69 The Journal, "Leaked emails show Irish Defence Forces held talks with controversial hacking company", 8 July 2015. Available at: http://www.thejournal.ie/irish-defence-forces-hacking-team-2206527-Jul2015/
70 See: https://www.hackingteam.it/images/stories/galileo.pdf

58. Following these relations, a spokesperson said "*The Defence Forces confirms that no services were purchased from the company in question*".[71] However, it is not clear whether the Irish state uses any other form of malware for surveillance purposes and in any event it is remarkable that a state authority was attempting to purchase malware which it would be illegal to use under Irish law. No Irish surveillance law permits the use of malware for this purpose, which would constitute the crimes of unauthorised use of a computer and criminal damage to data.[72] This incident therefore suggests either that the Permanent Defence Force is unaware of its legal obligations, or else is operating on the basis of a secret interpretation of the law to permit the use of malware. In either event, the Irish state must clarify as a matter of urgency the legal rules against the use of malware in this way.

71 The Independent, "Military Chiefs: No software bought from hacker firm", 10 July 2015, Available at: http://www.independent.ie/business/technology/military-chiefs-no-software-bought-from-hacker-firm-31366035.html

72 For a summary of these offences see T.J. McIntyre, "Computer Crime in Ireland: A Critical Assessment of the Substantive Law," Irish Criminal Law Journal 15, no. 1 (2005): 13; T.J. McIntyre, "Cybercrime in Ireland," in Cybercrime and Security, ed. Pauline C. Reich (Oxford University Press, 2008).

VII. Recommendations

We recommend that the Government of Ireland:

1. Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards including the principles of legality, proportionality and necessity;
2. Take the necessary measure to ensure that all interception activities – including access to stored communications – are subject to prior judicial authorisation;

3. Update the law to criminalise the interception without legal authority of all communications – including internet communications – and to address the particular problems of IMSI catchers and surveillance malware;

4. Provide effective oversight over the surveillance practices of all state agencies, including the establishment of a dedicated body to oversee surveillance on an ongoing basis and with the technical and legal expertise necessary for that purpose;

5. Repeal the data retention law in order to ensure compliance with the Charter of Fundamental Rights and other international standards in light of the CJEU judgment against data retention; and

6. Take positive steps to protect the right to privacy of those within its territory and jurisdiction, endeavouring to maintain the integrity of communications systems and safeguarding against illegitimate access of those systems.