Data Retention in Ireland: Privacy, Policy and Proportionality[1]

TJ McIntyre
tjmcintyre@ucd.ie
Lecturer in Law, University College Dublin

Published as McIntyre, TJ, Data Retention in Ireland: Privacy, Policy and Proportionality, Computer Law & Security Review, Volume 24, Issue 4, 2008, Pages 326–334.

Abstract

The growth of data retention in Europe has been marked by an interplay between national laws and European developments such as the Telecommunications Privacy Directives[2] and the Data Retention Directive.[3] This article examines the Irish dimension to that growth, outlining how the Irish State has pursued data retention simultaneously by way of domestic law and European initiatives, and considering whether the resulting policy has had the effect of undermining both the right to privacy and the principle of democratic oversight.

1. Introduction

The Irish State has been an early pioneer in the use of telecommunications to track the movements and communications of the population, and (together with France, Sweden and the United Kingdom) has been one of the main proponents of data retention laws at European level.[4]

Ireland has also seen resistance to these developments, with the civil rights group Digital Rights Ireland[5] bringing the first litigation to challenge domestic and European data retention laws on fundamental rights grounds. (Litigation which has now been matched by a constitutional challenge in Germany.[6])

---

[1] This article is based on a paper given at the Irish Centre for European Law / ERA Conference, "The Impact Of The Fight Against Terrorism On EU Law", 2 November 2007 and also on a previous article "Data Retention: History and Developments" (2007) 2 *Data Protection Law and Policy* 14. Disclosure: the author is chairman of Digital Rights Ireland and is involved in lobbying against data retention in Ireland.

[2] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

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

[4] Lillington, "Government support for data plan at odds with own policies", *The Irish Times,* 3 August 2001. Council document 8958/04, "Proposal for a Framework Decision on Data Retention", 28 April 2004.

[5] http://www.digitalrights.ie.

[6] See Deutche Welle World, "Germans file mass lawsuit against sweeping data retention law", 31 December 2007, available at http://www.dw-world.de/dw/article/0,2144,3025009,00.html.

However, while the international dimensions of data retention have been well covered[7], there is very little literature on the data retention issue as it has developed in Ireland.[8] The aim of this article is to fill that gap by offering an Irish perspective on the broader European debate. As such this article will not address in detail the history of the Data Retention Directive[9], which has been well covered elsewhere.[10]

2. Defining data retention

The terminology used in this area – "data retention" – is unfortunate, suggesting something rather technical and dull. It might be preferable to adopt the language used by Solove who talks of technology creating "digital dossiers".[11] As technology comes to permeate more and more aspects of everyday life, our interaction with that technology leaves a trail of digital footprints which record almost everything we do. In particular, our mobile phones operate as tracking devices, creating a detailed account of our movements and the persons to whom we talk.

Similarly records of our web browsing and email can reveal in great detail the newspapers we read, the stories we choose to follow, the people with whom we communicate and even information about our health, our finances, our politics or our sexual preferences. Aggregated together, these details create a comprehensive digital dossier about every individual.

These digital footprints have, until now, generally been ephemeral. The intermediaries processing these details have been obliged by general data protection law not to store this information unless it is necessary to do so, and in any event not to retain the information for longer than necessary for the purpose for which it is collected. Data retention laws change this. By compelling intermediaries to store information which would otherwise be deleted they in effect outsource surveillance from the state to the private sector by requiring telecommunications companies to track and log the activities of all their customers, judge, jurist and jailbird[12] alike.

---

[7] E.g. Rauhofer, "Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union", (2006) 3:4 *SCRIPT-ed* 322, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/rauhofer.asp; Bowden, "CCTV for inside your head" (2002) 8(2) *Computer and Telecommunications Law Review* 21; Walker and Akdeniz, "Anti-terrorism laws and data retention: War is over?", (2003) 54(2) *Northern Ireland Legal Quarterly* 159; Rowland, "Data Retention and the War Against Terrorism – A Considered and Proportionate Response?", 2004 (3) *The Journal of Information, Law and Technology*, available online at http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_3/rowland/; Vilasau, "Traffic Data Retention v Data Protection: The New European Framework" (2007) 13(2) *Computer and Telecommunications Law Review* 52.

[8] With the exception of Kelleher, *Privacy and Data Protection Law in Ireland* (Dublin, Tottel, 2006), Chs. 17 and 18.

[9] Directive 2006/24.

[10] E.g. Kosta and Valcke, "Retaining the data retention directive" (2006) 22 *Computer Law and Security Report* 370.

[11] Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York, NYU Press, 2004).

[12] A recent scandal was prompted by the revelation that a caller to a popular radio programme was in fact a convict in Ireland's maximum security prison calling from his cell on a contraband mobile phone. See Lally, "McDowell concerned over prisoner's call" *The Irish Times*, 2 May 2007.

This is, it should be noted, qualitatively different from traditional police powers – instead it provides for pre-emptive surveillance of the entire population on the basis that some of that population might at some stage commit some crime or otherwise come to the attention of the authorities and that this information might then be of assistance.[13]

3. Domestic legislative background

Modern Irish telecommunications law dates from 1983, when legislation was introduced to transfer telecommunication services from central government to a separate State-owned company, Telecom Éireann.[14] That legislation prohibited the interception of communications – "interception" was, however, defined narrowly so as to mean "listening to or recording" a telecommunication message, excluding what was then referred to as "metering", which today would be described as the gathering and disclosure of telephone traffic and location data.[15]

Metering was, therefore, largely unregulated, and remained so until 1993, when new legislation was passed in the wake of a scandal involving the Taoiseach (Prime Minister) and a senior government minister[16] who had colluded in the extensive tapping of journalists' telephones.[17] That legislation largely focused on interception, but also dealt with metering and provided that requests to Telecom Éireann for metering information were to be in writing, and signed by a senior member of the Garda Siochána (police force) or military officer.[18]

This, however, still left metering without any real oversight or control. In particular (and by contrast with interception):

- There was no requirement for any prior independent authorisation before metering could be carried out;
- There was no oversight system in place to monitor the use of metering;[19]
- There was no limitation on the period for which metering could be used;
- Metering was not restricted to serious offences;
- There was no requirement that the use of metering be either necessary or proportionate in the circumstances of the individual case; and
- There was no limitation of the length of time for which traffic data could be retained.

---

[13] This is characteristic of what Marx has termed "the new surveillance". See Marx, *Undercover: Police Surveillance in America* (Berkeley, Ca., University of California Press, 1988), Ch. 10.
[14] Postal and Telecommunication Services Act 1983. See the discussion in Hall, *The Electronic Age: Telecommunication in Ireland* (Dublin, Oak Tree Press, 1993), Ch. 9.
[15] Section 98. See Hall, *op. cit*., Ch. 28 and Kelleher, Chs. 17 and 18.
[16] Interception of Postal Packets and Telecommunications Act 1993.
[17] The journalists in question brought legal proceedings against the State, resulting in the decision in *Kennedy and Arnold v. Ireland* [1987] IR 587. See Collins, "Telephone Tapping and the law in Ireland" (1993) *Irish Criminal Law Journal* 31.
[18] Section 98(2A) of the Postal and Telecommunication Services Act 1983 as amended.
[19] Sections 8 and 9 of the 1993 Act, dealing with the role of the Designated Judge and the Complaints Referee, were limited in their scope to "interceptions" only, which that Act defines as "listening to" or "recording of" a telecommunications message. The Court of Criminal Appeal appeared to misconstrue these sections in *People (DPP) v Colm Murphy* [2005] IECCA 1, [2005] 2 IR 125 where it was suggested (at paragraph 97) that these safeguards did apply to metering also.

This position remained essentially unchanged even after deregulation of the Irish telecommunications market in the late 1990s – instead, the existing law was simply extended to the newly licensed operators.[20]

The first Telecommunications Privacy Directive[21] should have changed this. It required that as a general rule, traffic data must be erased or made anonymous as soon as the communication ends, and therefore implicitly prohibited blanket data retention.[22] However, Ireland did not implement that Directive until May 2002, three years late, by which time it had been overtaken by events.[23]

In the meantime, while telecom operators were not obliged to retain traffic data, they could do so if they wished, subject only to the general data protection principle that such information should not be "irrelevant and excessive" and should not be kept for longer than necessary for its purpose.[24]

4. Data retention revealed

In November 2001 *Irish Times* journalist Karlin Lillington revealed that Irish telephone companies were holding telephone traffic and mobile phone location data for six years, and were making that information available to the police on request.[25] When challenged, they gave two separate justifications – that it was necessary to keep the information until the contractual limitation period (6 years) expired[26], and that they were "waiting to see whether pending telecommunications amendments … would require them to retain locator data for future investigations".[27]

---

[20] Section 7 of the Postal and Telecommunications Services (Amendment) Act, 1999.
[21] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[22] See the discussion in Rauhofer, "Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union", (2006) 3:4 SCRIPT-ed 322, available online at http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/rauhofer.asp where it is pointed out that "Although Art. 14(1) of the same Directive allowed member states to derogate from that obligation and generally to restrict the data subject's right to privacy, this was only possible in very limited circumstances, namely "when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system". The UK government had not made use of the derogation when implementing the Directive since there was substantial legal doubt about whether a blanket data retention requirement would fall within the provisions of Art. 14(1)."
[23] European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002 (S.I. No. 192 of 2002).
[24] Section 2(1) Data Protection Act 1988,
[25] "Irish Know Where You've Been", *Wired News* 9 November 2001, available at http://www.wired.com/news/privacy/0,1848,48251,00.html . This followed similar revelations in the UK – see, e.g., Miller and Kelso, "Liberties Fear Over Mobile Phone Details" *The Guardian,* 27 October 2001.
[26] Statement by Joe Meade, Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data on 24 February 2003, available at http://www.dataprivacy.ie/viewdoc.asp?DocID=224
[27] "Irish Know Where You've Been", *Wired News* 9 November 2001, available at http://www.wired.com/news/privacy/0,1848,48251,00.html

The Data Protection Commissioner[28] was not persuaded by these arguments and took the view that a six year retention period was excessive and therefore incompatible with the Data Protection Act 1988 and the Telecoms Privacy Directive.[29] Despite pressure from the Department of Justice (which sought a three year retention period for security purposes), the Data Protection Commissioner directed the telephone companies to retain data for no longer than six months.[30]

In order to sidestep that decision, the Government in April 2002 issued[31] a secret direction, requiring telecommunications operators to retain all traffic data (including mobile phone location data) for three years. The direction also required operators to keep the existence of the direction secret.[32]

Being secret, this direction was not subject to public scrutiny. It was, however, challenged in private correspondence by the Data Protection Commissioner. He took the view that the direction was *ultra vires*, was an attempt to usurp the law making powers of the Oireachtas (Parliament), amounted to a significant restriction of the right to privacy, lacked the character of law (as required by article 8 of the European Convention on Human Rights), and was in breach of the provisions of the first Telecommunications Privacy Directive.[33] He also claimed that it was unacceptable that such an invasive and far reaching law should be made in a way designed to evade Parliamentary oversight or judicial review.[34]

There was considerable weight to each of these points.

The supposed power to make such a direction was contained in section 110 of the Postal and Telecommunications Services Act, 1983, which provides that telecoms operators might be directed "to do (or refrain from doing) anything which [the Minister] may specify from time to time as necessary in the national interest". This provision had been relied upon in the past as the legal basis for interception of communications in individual cases – it had never, however, been suggested that it provided a legal basis for mass surveillance of all users. Indeed, if section 110 could be read as conferring such an wide discretion then it would appear to be in breach of the Irish Constitution's prohibition on delegation of legislative power, which requires that delegated powers should not go beyond merely "filling in the details of principles and policies already articulated" in the parent legislation.[35]

---

[28] Then Joe Meade.
[29] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[30] Statement by Joe Meade, Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data on 24 February 2003, available at http://www.dataprivacy.ie/viewdoc.asp?DocID=224
[31] Under s110(1) of the Postal and Telecommunications Services Act, 1983. The direction was issued by the Minister for Public Enterprise, Mary O'Rourke.
[32] Lillington, "Court threat for State over data privacy", *The Irish Times* 26 May 2003. Statement by Joe Meade, Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data on 24 February 2003, available at http://www.dataprivacy.ie/viewdoc.asp?DocID=224
[33] Lillington, "Court threat for State over data privacy", *The Irish Times,* 26 May 2003.
[34] Lillington, "Secret data traffic direction may break law", *The Irish Times*, 30 March 2003.
[35] Hogan and Whyte, *Kelly: The Irish Constitution* (4th ed., 2003) at 248, summarising the line of cases starting with *Cityview Press v. AnCO* [1980] IR 381.

The direction also appeared to breach Article 8 of the European Convention on Human Rights, which provides that "[t]here shall be no interference by a public body with the exercise of this right except such *as is in accordance with the law*". The phrase in italics has been held by the European Court of Human Rights to mean that any interference with the right to privacy must be authorised by a law which is "adequately accessible" to the citizen, and "formulated with sufficient precision" so as to provide "a measure of legal protection in domestic law against arbitrary interferences by public authorities".[36] In relation to secret surveillance it also means that there must be a system of "adequate and effective guarantees against abuse" including effective supervisory control by an independent body.[37] The entirely secret regime established by the 2002 direction – lacking as it did any oversight mechanism –failed on all grounds.

The Commissioner therefore threatened to judicially review the direction unless these concerns were met – insisting that if the Government insisted on imposing a data retention regime, then it must do so via primary legislation.[38] The Minister for Justice (Michael McDowell) agreed to introduce stand-alone legislation to this effect by Autumn 2002 and promised that the direction would be a temporary "holding measure" until the legislation could be passed.[39]

5. Proposed legislation and consultation

In drafting this legislation, the Department of Justice consulted only the police. There was no contact with the industries affected (on the basis that the Department "knew that they would be co-operative") or the public. In isolation, the Department produced a draft Bill – which went beyond the original direction by proposing to extend data retention to Internet use.[40] Only when the existence of the ministerial direction and draft legislation was revealed did the Department begin making limited consultations on the matter.[41]

This began in February 2003 by means of a private, unpublicised industry event which was initially planned to exclude even the Data Protection Commissioner. The Commissioner was eventually added to the list of speakers and gave voice to his dissatisfaction with the confidential ministerial direction. He insisted that the Oireachtas should "fully debate" the privacy concerns and enact any legislation "at an early date" – in effect reiterating his prior threat to bring judicial review proceedings unless authorising legislation was passed.[42]

Following this event, the Department changed tack and set up a website to facilitate a consultation on data retention, which outlined the proposed legislation.[43] Opposition grew, with the Irish Council for Civil Liberties, the Electronic Privacy Information Centre, the International Chamber of Commerce and technology lobby ICT Ireland

---

[36] *Malone v.United Kingdom* (1984) 7 EHRR 14 at para. 68.
[37] *Klass v. Germany* (1978) 2 EHRR 214 at paras. 49-55.
[38] Lillington, "Court threat for State over data privacy", *The Irish Times,* 26 May 2003.
[39] Lillington, "Data retention plans cause considerable unease", *The Irish Times*, 23 June 2003.
[40] Lillington, "Bill would allow personal data to be stored for 4 years", *The Irish Times*, 28 November 2002.
[41] Lillington, "Consultation over data Bill is a farce", *The Irish Times*, 21 February 2003.
[42] Lillington, "Consultation over data Bill is a farce", *The Irish Times*, 21 February 2003.
[43] That site is still online and can be accessed via http://www.justice.ie.

expressing concern and advocating the alternative, more privacy friendly system of "data preservation".[44] Industry concerns of "massive costs" were shared by the Department of Communications, Marine and Natural Resources, which clashed with Justice, opposing retention because of the impact it would have on Ireland's competitiveness. The Department of Communications went so far as to argue that "businesses may also have greater concerns regarding confidentiality of sensitive business communications" and suggested that the retention regime should be limited to private citizens.[45]

6. Moving data retention to Europe

At some point in late 2003 or early 2004, despite having missed the Autumn 2002 date initially promised to the Data Protection Commissioner (and despite the Commissioner having threatened on three separate occasions to commence proceedings[46]), the Department of Justice appeared to shift its focus from a domestic data retention Bill towards pushing for mandatory data retention at an EU level.

In April 2004, during its Presidency of the EU and shortly after the Madrid train bombings, Ireland proposed[47] a Framework Decision on Data Retention and letters were sent by the Department to those involved in the consultation process, indicating that it would now wait for legislation to be enacted at European level.[48]

Some observers suggested that this was an attempt to avoid democratic scrutiny of the proposals.[49] As Karlin Lillington put it:

> "A cunning plan, then. The Irish Government proposes the directive for the EU, and … the Department of Justice can then duck criticisms of its own policy in support of such legislation here – although it has failed to produce even the heads of a Bill in two years, nicely keeping its intentions out of the public and Oireachtas eye."[50]

These suspicions were exacerbated by the form of the Irish proposals – by proceeding by way of a Framework Decision, the matter would be determined by the Council, excluding any real input from the European Parliament.

7. Data retention comes back to Ireland

At this point, it appeared that the issue had moved to Europe. It was with some surprise, then, that Irish observers learned in early 2005 that data retention provisions had been tacked on to an unrelated Bill and had been passed into domestic law almost without debate.[51] Karlin Lillington was trenchant in her criticism at the time:

---

[44] Lillington, "Court threat for State over data privacy", *The Irish Times,* 26 May 2003; Lillington, "Lobby condemns data storage plans", *The Irish Times*, 9 June 2003.
[45] Lillington, "Data retention plans cause considerable unease", *The Irish Times*, 23 June 2003. Lillington, "Departments at odds on Data Retention Bill", *The Irish Times*, 27 June 2003.
[46] Lillington, "McDowell is hypocritical on the issue of privacy – Freedom of Information gutted while Government privacy is sacrosanct", *The Irish Times*, 10 October 2003.
[47] Council document 8958/04, "Proposal for a Framework Decision on Data Retention", 28 April 2004.
[48] Lillington, "Back door policy for data retention wrong", *The Irish Times* 30 July 2004; Lillington, "Government on EU data retention mission", *The Irish Times,* 7 May 2004.
[49] Lillington, "European data law attracts serious opposition", *The Irish Times*, 5 October 2005.
[50] Lillington, "Back door policy for data retention wrong", *The Irish Times* 30 July 2004.
[51] As Part 7 of the Criminal Justice (Terrorist Offences) Act, 2005.

> "Appalling and deeply cynical about the democratic process. That's how you describe a government that first slaps a broad semi-surveillance order secretly on its own population through a cabinet direction condemned by international privacy organisations, and then turns it into law three years later through a last minute amendment to a Bill "debated" by an empty Dáil…
>
> The amendment came in with such stealth that even TDs [members of parliament], business leaders and privacy advocates who had been following the issue closely were caught unawares. No doubt the whole point of the amendment, of course. Mr McDowell had repeatedly promised, on radio, television and in print, a full Bill dealing with data retention, which would be broadly and openly debated in both houses of the Oireachtas…
>
> Last week, I spoke to several industry organisations and business leaders who expressed astonishment that data retention had been passed in a Bill they had heard nothing about, without any consultation on the amendment with industry bodies. Even the few groups that had been consulted as part of the slow progress towards the long-promised Bill were shocked, having had no idea that data retention had been quickly popped into another bill."[52]

Why the sudden urgency? In January 2005 the Data Protection Commissioner had finally tired of the failure to respond to his warnings and had directed telecommunications providers that, from May 5th, they must delete traffic data which was more than six months old – in effect, treating the ministerial direction as of no legal effect and inviting the providers to decide which direction to follow.[53] Coincidentally, in January 2005 the admissibility of traffic data as evidence was first raised before the Irish courts (in *People (DPP) v. Murphy*[54]), which appears to have convinced the Government that a proper statutory basis for retention, including oversight and safeguards, was necessary to ensure admissibility.[55]

The proposed Framework Decision had by this point run into difficulties, particularly as regards its legal basis, with the Commission arguing that it was a measure which properly belonged under the First Pillar – as a result there was no possibility that the Department could succeed in legalising data retention before May by means of European law. Or, as the Minister put it: "There is no EU cavalry coming down the hill to help me. I must sort out this conflict."[56]

Consequently, data retention provisions were attached to the final stages of the Criminal Justice (Terrorist Offences) Bill – putting in place a mandatory data retention regime in respect of telephone traffic and location data, with a three year retention period, and establishing oversight of the data retention system – and rushed through the Dáil and Seanad in two short sessions.

---

[52] Lillington, "McDowell's sneaky data law heralds surveillance state", *The Irish Times*, 25 March 2005.
[53] See the discussion at 598 *Dáil Debates* 23 February 2005.
[54] [2005] IE CCA 1. That decision held that telephone traffic data was admissible in evidence and its use did not violate Article 8 of the European Convention on Human Rights. In reaching this conclusion, however, it relied on the purported existence of judicial safeguards and oversight. For the reasons given earlier, this author believes that the decision was mistaken in this regard: lacking proper oversight, the data retention practices in place prior to 2005 would not have met the standards set out in, *inter alia*, *Malone v United Kingdom* (1985) 7 EHRR 14.
[55] Hosein, "Privacy and Cyberspace: Questioning the Need for Harmonisation", paper delivered at the ITU WSIS Thematic Meeting on Cybersecurity, 28 June – 1 July 2005, and available online at http://www.itu.int/osg/spu/cybersecurity/2005/material.html.
[56] 179 *Seanad Debates*, 3 February 2005.

In justifying this tactic, the Minister relied on three main arguments. First, it was argued that the urgency involved ruled out the introduction of the promised stand-alone Bill – an argument which would have been more persuasive had the exigency not been created by the earlier delay of the Department in dealing with the Data Protection Commissioner's warnings. Moreover, had time constraints been a legitimate reason to proceed in this way, it would have been appropriate to treat the legislation as a holding measure only. However, opposition amendments to introduce a sunset clause were rejected at both Dáil (Lower House) and Seanad (Upper House) stages on the basis that "international terrorism is a semi-permanent threat and, therefore, I will not put in place temporary legislation to deal with it."[57]

Secondly, the argument was made that Ireland's international obligations required that data retention be implemented. It is not clear what was meant by this (unless it was a misreading of the effect of the second Telecommunications Privacy Directive[58]) but Ireland was subject to no such legal obligation.[59]

Finally, it was suggested that the changes made merely regularised the existing law – a view which had already been rejected by the Department of Communications, which had previously pointed out that "the imposition of a three-year data retention period for the purposes of criminal investigation, etc., is an entirely new concept and should not be portrayed as a mere amendment to existing procedures."[60]

8. The Criminal Justice (Terrorist Offences) Act 2005

The current Irish law on data retention is therefore contained in Part 7 of the 2005 Act, which allows the Commissioner of the Garda Siochána to require telecommunications providers to retain traffic and location information for a period of three years for the purposes of (a) the prevention, detection, investigation or prosecution of crime (including but not limited to terrorist offences), or (b) the safeguarding of the security of the State.[61]

Access to this information is on the same basis as existed under the 1993 Act – an army officer or a member of the police force of sufficient rank can make an access request without any need for external approval.[62] The oversight regime established by the 1993 Act is also extended to data retention – for the first time, complaints

[57] 179 *Seanad Debates*, 3 February 2005.
[58] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. That Directive permitted (but did not require) blanket data retention.
[59] Lillington, "McDowell's sneaky data law heralds surveillance state", *The Irish Times*, 25 March 2005. Hosein, "Privacy and Cyberspace: Questioning the Need for Harmonisation", paper delivered at the ITU WSIS Thematic Meeting on Cybersecurity, 28 June – 1 July 2005, available online at http://www.itu.int/osg/spu/cybersecurity/2005/material.html.
[60] Lillington, "McDowell's sneaky data law heralds surveillance state", *The Irish Times*, 25 March 2005.
[61] Section 63.
[62] Section 64.

regarding disclosures can be made to the Complaints Referee[63], and the operation of the data retention system is to be kept under review by the Designated Judge.[64]

9. Criticisms of the 2005 Act

The 2005 Act is certainly an improvement on the previous situation, insofar as it reduces the retention period and introduces an element of oversight. However, significant flaws remain.

9.1 Proportionality

It must be doubted whether a law which requires the surveillance of all users, at all times, can be considered to be necessary or proportionate under Article 8 of the European Convention on Human Rights. This is particularly the case given that in 2001 the Council of Europe Cybercrime Convention achieved international agreement on a less invasive "data preservation" or "quick freeze" system, which would serve the need of preserving evidence in individual cases without the blanket storage of information on all users.[65] This system has, however, never been tried in Ireland. The comments of the Article 29 Working Party[66] in respect of the Directive would also appear to be appropriate in this context:

> The powers available to law enforcement agencies in the fight against terrorism must be effective, but they cannot be unlimited or misused. A proportionate balance must be struck to ensure that we do not undermine the kind of society we are seeking to protect. This balance is especially necessary when forcing communication service providers to store data that they themselves have no need for. In this manner, one could eventually achieve the unprecedented, continued, pervasive monitoring of all kinds of communication and movement of the totality of citizens in their daily life. A huge amount of information would be stored that is actually useful for investigational purposes in a limited number of cases.
>
> Consideration should also be given to the circumstance that such a sweeping data retention obligation impacts on some communications that raise delicate issues in connection with certain categories of professional and/or investigational secrecy, or certain activities by particular institutions, that are protected specifically by the law.
>
> For this reason, for some years now the view of both the Article 29 Working Party and the Conference of European Data Protection Authorities has been firm and clear. Upon several occasions since 1997, the Working Party and the European Conference have questioned the necessity of general data retention measures.

9.2 Authorisation

The Act does not change the position regarding authorisation for access to data – this is still an internal matter for a senior police officer with no prior independent or judicial approval required.

9.3 No limitation to serious crime

[63] Section 65.
[64] Sections 66 and 67.
[65] Council of Europe. Convention on Cybercrime, ETS No.185.
[66] Opinion 4/2005.

As before (and despite the reference in the title of the Act to "terrorist offences") the data can be accessed in the case of any crime, however trivial.[67] There is still no requirement that the use of traffic data be either necessary or proportionate in the circumstances of the individual case – as such, there is nothing to stop indiscriminate access to data or "fishing expeditions". This problem is exacerbated by the lack of any provision for cost reimbursement for the telecom operators (either for the initial storage or for the administrative costs of responding to police requests) – there is, therefore, not even a financial incentive to be selective in the amount of requests made or the amount of data sought. There are no publicly available figures on the use made of data retention information. However, the Assistant Data Protection Commissioner[68] recently announced that the police were making approximately 10,000 requests per year for telecommunications data.[69] This suggests that use of data retention is not being limited to serious crime or terrorist offences.

9.4 Data available for civil proceedings

A further problem with the Act is that it does not limit access to this data to law enforcement – section 64 allows the data to be accessed "in accordance with a court order … [or] for the purpose of civil proceedings in any court". Consequently, it is safe to predict that parties to civil litigation will eagerly seek discovery of this data – and the oversight mechanisms in the Act do not appear to apply to such access.

9.5 Length of retention period

The three year retention period is an improvement when compared with the previous six year period – but no reason was given as to why three years was necessary. Indeed, the Department of Communications in correspondence with the Department of Justice had made precisely this point – that there was no "particular justification for this period or any statistical information that would indicate this to be the optimum period based on previous experience of gardaí in investigations".[70] The three year period also disregards the findings of the Article 29 Working Party which had stated[71] in 2004 that:

> "analysis carried out by telecommunications companies in Europe reveal that the biggest [*sic*] amount of data demanded by law enforcement were not older than three months. This shows that longer periods of retention are clearly disproportionate."

9.6 Oversight mechanism

The 2005 Act extends the duties of the Designated Judge under the interception regime to the retention and disclosure system, and he[72] is given the power to

---

[67] Lillington, "New data retention law raises fears of abuse", *The Irish Times*, 14 April 2006.
[68] Gary Davis.
[69] Speaking at the University College Cork Law Society Conference on Defamation and Privacy, 30 November 2006. This is higher than the "hundreds of requests" per month previously indicated by Joe Meade's successor as Data Protection Commissioner, Billy Hawkes in Lillington, "New data retention law raises fears of abuse", *The Irish Times*, 14 April 2006.
[70] Lillington, "McDowell's sneaky data law heralds surveillance state", *The Irish Times*, 25 March 2005.
[71] Opinion 9/2004.
[72] All holders of the office to date have been male.

investigate any case in which a disclosure request was made and must make an annual report to the Taoiseach which is laid before the Oireachtas.[73] Similarly, the powers of the Complaints Referee are extended to the disclosure system.[74]

However, this oversight system has been almost entirely opaque from the outset. The annual reports of the Designated Judge – since that position was created in 1993 – have consisted every year of no more than a single line stating that the operation of the Act has been kept under review and its provisions are being complied with. There has, for example, been no discussion of what steps were taken to keep the operation of the Act under review; whether individual files were reviewed; the volume of surveillance being carried out; and whether mistakes were made in carrying out surveillance (such as the targeting of the wrong individual or number) and, if so, what steps were taken to safeguard against such mistakes in future. There is similarly no publicly available report of the Complaints Referee indicating what complaints, if any, have been made and/or upheld.

This may be contrasted with the most recent Annual Report of the UK Chief Surveillance Commissioner[75] which reveals, amongst other things, that 23,628 authorisations for directed surveillance were granted to law enforcement agencies; 60 different law enforcement agencies were inspected during the year; most of those agencies "have yet to introduce effective arrangements for the handling, storage and destruction of material obtained through the use of covert surveillance"[76]; and that unauthorised surveillance continues to take place where the authorising officers fail to understand what form of surveillance they can permit and in what circumstances.[77]

Moreover, the scope of the investigation which the Designated Judge can carry out is limited. He may "ascertain whether the Garda Síochána and the Permanent Defence Force are complying with" the 2005 Act[78] – but there is no power to ensure that other public bodies which may have investigatory functions – such as the Revenue – are doing likewise, nor is there any power on the part of either the Designated Judge or the Complaints Referee to investigate possible abuses within the telecommunications providers themselves.

9.7 Security measures

Contrary to the recommendation[79] of the Article 29 Working Party that "[m]inimum standards should be defined concerning the technical and organisational security measures to be taken by providers", the 2005 Act does not prescribe any security measures for data retained by telecommunications operators.

10. Irish opposition to European data retention proposals

[73] Section 67.
[74] Section 65.
[75] The 2005/2006 Report, available at http://www.surveillancecommissioners.gov.uk/docs1/annualreport200506.pdf.
[76] Para 8.6.
[77] Para 8.11.
[78] Section 67.
[79] Opinion 3/2006.

In 2005, with domestic data retention a *fait accompli*, attention shifted back to the proposed European laws. There was increasing opposition in Ireland to data retention – motivated, at least in part, by the stealthy way in which the 2005 Act had been passed. Although the Irish Council for Civil Liberties had been active in opposing data retention, it was felt that it would be desirable to have a group which could focus specifically on civil liberties and technology issues and Digital Rights Ireland was formed in October 2005 with (amongst other things) the specific purpose of fighting data retention.

Ironically, however, the Department of Justice itself soon came to oppose European data retention measures. Its initial enthusiasm for a European response waned once it became clear that the proposed Framework Decision was to be replaced with a First Pillar Directive (as a result of Commission intervention, opposition from the European Parliament, doubts about the legal basis for the measure, and a lack of unanimity in the Council). Motivated (apparently) by a desire to maintain the national veto in this area, the Minister for Justice announced that data retention should be dealt with under the Third Pillar only, and indicated that Ireland (supported by Slovakia) would vote against and would challenge the Directive if passed.[80]

At first glance, this assisted the civil rights campaign against the Directive – if the Government was going to challenge the Directive then even MEPs from the Government parties had no reason to support it. All Irish MEPs were contacted and urged to vote against the Directive. The result was mixed – of thirteen Irish MEPs one[81] voted in favour, three[82] against, while nine[83] either abstained or were absent. While this may be due to confusion caused by the change of heart of the Government, it is notable that the majority of Irish MEPs appeared to have no views about the introduction of mass surveillance or indeed about the legal basis for the Directive.

11. Legal challenges

After the passing of the Directive the Irish Government followed through on its threat and in July 2006 commenced an Article 230 challenge in the European Court of Justice alleging that the Directive had been adopted using the wrong legal basis.[84] This challenge is, however, procedural only – it does not challenge the principle of data retention but merely the legal basis on which it was adopted.

In September 2006 Digital Rights Ireland started a more far reaching action before the Irish High Court.[85] This action challenges both the Directive and also Ireland's

---

[80] "Data Retention Directive adopted by JHA Council*", EDRI-gram* - Number 4.4, 1 March 2006. Available at http://www.edri.org. Some reports suggest that the primary motivation was to keep Ireland's longer retention period – see, e.g., Lillington, "EU Directive spells end to e-mail, internet privacy", *The Irish Times*, 13 January 2006 – though this seems unlikely given the option which the Directive allows for longer periods.

[81] Proinsias De Rossa.

[82] Mary Lou McDonald, Gay Mitchell, Marian Harkin.

[83] Eoin Ryan, Liam Aylward, Avril Doyle, Mairead McGuinness, Simon Coveney, Brian Crowley, Kathy Sinnott, Jim Higgins, Sean O' Neachtain.

[84] Case C-301/06, 2006 OJ (C 237) 5.

[85] Case 2006 No. 3785P. Press release available at http://www.digitalrights.ie/2006/09/14/dri-brings-legal-action-over-mass-surveillance/ and pleadings available at: http://www.mcgarrsolicitors.ie/2006/09/14/digital-rights-ireland-ltd-statement-of-claim/.

domestic data retention practices (including the 2005 Act), and does so on the basis that those laws are not merely procedurally flawed but are also in breach of the right to privacy guaranteed under the Irish Constitution[86] and Article 8 of the European Convention on Human Rights.[87] It is also argued that data retention, by monitoring all communications, will have a chilling effect on the Constitutional and Convention rights to freedom of expression and association.[88] In addition, the action argues that the tracking and storing of the movements of any person carrying a mobile telephone amounts to an interference with the unenumerated right to travel recognised under the Constitution[89] insofar as it establishes a system of state-mandated surveillance of the movements of the overwhelming majority of the population. The action alleges that these infringements of personal rights are neither proportionate nor necessary in a democratic society.

At the time of writing the action remains at the interlocutory stages before the High Court, where the Irish Human Rights Commission has made an application to the court for permission to intervene in the case as an amicus curiae.[90] In the context of that application, the State has also indicated its intention to challenge the *locus standi* of Digital Rights Ireland as a preliminary matter. Both applications have yet to be ruled on by the court.

12. Conclusion

The history of data retention law in Ireland has been marked by an absence of democratic debate and oversight. The 2002 Direction in particular stands out as an attempt to make law in secret coupled with an attempt to stymie any public debate or judicial review by directing the recipients of the Direction to remain silent as to its existence. Similarly, when finally compelled by the Data Protection Commissioner to proceed by primary legislation, the Department of Justice did so in 2005 without notice, in a way calculated to exclude any public scrutiny, and ignoring its own express assurances that draft legislation would be published and debated. [91]

The Irish situation also appears to prove the truth of the point made by Privacy International, Statewatch and the American Civil Liberties Union (amongst others), that in the area of surveillance national governments are engaged in "policy laundering", that is to say: "pursuing policy in international institutions to then bring them back home under the guise of an international obligation, rendering Parliaments and Congresses powerless to object."[92] Indeed, the Minister's comment that "there is

---

[86] Article 40.3. See, e.g., *Kennedy and Arnold v. Ireland* [1987] IR 587.
[87] See, e.g., *Malone v.United Kingdom* (1984) 7 EHRR 14. This aspect of data retention is covered comprehensively in Breyer, "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11 *European Law Journal* 365.
[88] Article 40.6.1 of the Constitution and Articles 10 and 11 of the European Convention on Human Rights, respectively.
[89] See for example *State (M) v. Attorney General* [1979] IR 73.
[90] Lillington, "Alarm bells ring over data retention" *The Irish Times*, 7 December 2007. The role of the Commission in such matters is defined by section 8(h) of the Human Rights Commission Act 2000.
[91] Lillington, "We must row back on surveillance legislation", *The Irish Times,* 17 March 2006.
[92] Hosein, "Privacy and Cyberspace: Questioning the Need for Harmonisation", paper delivered at the ITU WSIS Thematic Meeting on Cybersecurity, 28 June – 1 July 2005, and available online at http://www.itu.int/osg/spu/cybersecurity/2005/material.html.

no EU cavalry coming down the hill to help me" is an unusually candid acknowledgement of this tactic.[93]

It is ironic, however, that in this case the process adopted in Europe proved to be substantially more transparent and open to public participation than the domestic process. National checks and balances have proven to be weak. Irish parliamentarians (with some notable exceptions) took scant interest in the issue – the passage of the 2005 Act was marked by little discussion of the data retention provisions, nor have parliamentarians objected to the manner in which they have been relegated to the sidelines in this debate (by the 2002 Direction, by attempting to take the matter to Europe, and ultimately by the introduction of data retention provisions as a last minute amendment). Irish MEPs have proved, for the most part, similarly indifferent – nine out of thirteen MEPs either abstained or were absent for the Directive vote, which does not suggest any great willingness to scrutinise this issue. The Data Protection Commissioner would appear to be the only Irish official who has offered an alternative viewpoint.

By way of contrast, the European debate was significantly more open, with Parliament, the Article 29 Working Party, the European Data Protection Commissioners collectively[94], and the European Data Protection Supervisor acting as institutional counterbalances to the Council and national executives. Even so, however, this was still described at the time as a rushed job apparently attributable to the desire on the part of the United Kingdom to see the matter adopted during their presidency.[95]

Against this background, the current challenges to data retention laws, in both Ireland and Germany, are all the more important. Given the hasty nature of these laws, it is past time that they were closely scrutinised as to their compatibility with fundamental rights. Perhaps most importantly the challenges offer an opportunity to reflect on the effect which pervasive surveillance might have on our society. The traditional concept of a reasonable expectation of privacy is one that depends, to a large extent, on changing conceptions of what is reasonable. Ubiquitous surveillance, if allowed to go unchallenged, may eventually become the norm.[96]

---

[93] In an Irish context, pursuing policy at an EU level will also have the effect of insulating any implementing law from domestic judicial scrutiny. See Article 29.4.10 of the Constitution which provides: "No provision of this Constitution invalidates laws enacted, acts done or measures adopted by the State which are necessitated by the obligations of membership of the European Union or of the Communities, or prevents laws enacted, acts done or measures adopted by the European Union or by the Communities or by institutions thereof, or by bodies competent under the Treaties establishing the Communities, from having the force of law in the State."

[94] At the European Data Protection Commissioners Conference (6/7 April 2000, Stockholm).

[95] For example, Gay Mitchell MEP commented at the time that: "I do not know why this proposal was rushed. The extremely accelerated legislation procedure has meant that there was little time for discussion, and translations were sometimes unavailable. There was also no time for a technology assessment or for a study on the impact on the internal market." *Parliamentary Debates*, 14 December 2005.

[96] Hosein, "Privacy as Freedom" in Jorgensen, ed., *Human Rights in the Global Information Society* (Cambridge, MA, 2006) puts it well: "Changing norms will change our regard for what are proportionate and necessary measures in a democratic society. Once it becomes expected that all information which is derived from our interactions in modern society is collected by default in the eventuality that we do wrong to someone or to the state, there is little ground for us to feel offended by

forced collection of DNA from all newborns, or the default fingerprinting of all individuals. After all, the logic goes, ‘Unless you have something to hide/fear, this data will never be used against you.”