Title	Implementing Information Privacy Rights in Ireland
Authors(s)	McIntyre, T.J.
Publication date	2015-11-22
Publication information	Egan, S. (ed.). International Human Rights: Perspectives from Ireland
Publisher	Bloomsbury Professional
Link to online version	https://www.bloomsburyprofessional.com/uk/international-human-rights-perspectives-from-ireland-
Item record/more information	http://hdl.handle.net/10197/10210

TJ McIntyre, "Implementing Information Privacy Rights in Ireland" in Suzanne Egan (ed.), *International Human Rights: Perspectives from Ireland* (Dublin: Bloomsbury, 2015), pp. 271-287.

Implementing Information Privacy Rights in Ireland

TJ McIntyre

UCD Sutherland School of Law and Digital Rights Ireland

tjmcintyre@ucd.ie

Introduction

How has the international human rights regime influenced privacy law in Ireland? The answer depends largely on which aspect of privacy we examine. International norms have been central to the development of the law in areas such as sexual identity, reproductive autonomy and family life.[1] From the 1980s onwards a series of high profile European Court of Human Rights ("ECtHR") cases including *Norris v. Ireland*[2], *Johnston v. Ireland*[3] and *A, B and C v. Ireland*[4] have forced domestic legislative change. Declarations of incompatibility under the ECHR Act 2003 have been granted in *Foy v. An t-Ard Chláraitheoir*[5] and *Donegan v. Dublin City Council*.[6] At a political level the Universal Period Review ("UPR") under the International Covenant on Civil and Political Rights ("ICCPR") has also resulted in intense scrutiny of issues such as abortion and transgender rights.[7]

However, when we turn to privacy as an information right – controlling the collection and use of personal data – the position has been entirely different. There have been no equivalent cases against Ireland before the Strasbourg court. The area has not featured to any extent in the UPR, where civil society has had other priorities. There is a significant body of national case law asserting information privacy rights – but even after the ECHR Act 2003 ("the 2003 Act") these cases have generally focused on privacy as a domestic constitutional right with little or no analysis of Article 8 ECHR.[8] The Government and Oireachtas have taken ECtHR jurisprudence into account in adopting criminal justice legislation but generally only in a limited way, passing laws only when forced to do so and confining the safeguards in those laws to the minimum necessary to resist challenge.[9]

---

[1] See e.g. Siobhan Mullally, "Debating Reproductive Rights in Ireland," *Human Rights Quarterly* 27 (2005): 78; Liam Thornton and Siobhan Mullally, "The Rights of the Child, Immigration and Article 8 in the Irish Courts," in *ECHR and Irish Law*, 2nd ed. (Bristol: Jordan Publishing, 2009).
[2] Application no. 10581/83, judgment of 26 October 1988.
[3] Application no. 96977/82, judgment of 18 December 1986.
[4] Application no. 25579/05, judgment of 16 December 2010.
[5] [2007] IEHC 470.
[6] [2008] IEHC 288.
[7] See e.g. Liam Thornton, "Human Rights in the Republic of Ireland," in *The Irish Yearbook of International Law*, ed. Jean Allain and Siobhán Mullally (Bloomsbury Publishing, 2011).
[8] See in particular *Atherton v. DPP* [2005] IEHC 429; *DPP v. Colm Murphy* [2005] IE CCA 1; *Gray v. Minister for Justice* [2007] IEHC 52; *White v. Morris* [2007] IEHC 107.
[9] Maria Helen Murphy, "The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases," *Irish Journal of Legal Studies* 3, no. 2 (2013): 65. A notable exception is the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 which was substantially amended during a drawn out legislative process to take account of concerns expressed by the Irish Human Rights Commission. See Ruadhan Mac Cormaic, "Reworked DNA Bill Seeks Balance between Privacy and Better Crime Detection," *The Irish Times*, September 12, 2013,

Until recently, therefore, international fundamental rights standards have had less impact in this area. However, this has changed significantly in a short time, to the extent that Ireland has now been described as an international "focal point" for privacy litigation.[10] In two landmark cases the Irish courts are at the forefront of human rights challenges to mass surveillance. The first, *Digital Rights Ireland v. Minister for Communications*[11], is an ongoing challenge to data retention – the collection and storage of information on the communications and movements of every citizen. It has already resulted in a decision of the Court of Justice of the European Union ("CJEU") striking down the Data Retention Directive as incompatible with the Charter of Fundamental Rights ("CFR") – the first time a directive has been invalidated on fundamental rights grounds.[12] The second, *Schrems v. Data Protection Commissioner*[13], is in form a judicial review of the Data Protection Commissioner but in substance challenges the legality of data transfers to the United States following Edward Snowden's revelations of indiscriminate NSA surveillance.[14] This has also been the subject of a preliminary reference to the CJEU.[15] While the CJEU has yet to rule in that reference, the issues it raises are of political and economic importance and a decision in favour of the plaintiff would have far reaching consequences for EU-US relations.[16]

In addition to these cases, personal information held in Ireland is now the topic of important litigation before the US courts. In a case currently before the Second Circuit Court of Appeals, Microsoft is challenging a warrant issued by a district judge in the Southern District of New York which requires it to produce customer data held in its Dublin data centre.[17] That case presents fundamental questions regarding extraterritorial jurisdiction over personal data and the relationship between EU and US law. It has already provoked strong criticism from the European Commission

---

http://www.irishtimes.com/news/ireland/irish-news/reworked-dna-bill-seeks-balance-between-privacy-and-better-crime-detection-1.1524274.

[10] Shane Darcy, "Battling for the Rights to Privacy and Data Protection in the Irish Courts," *Utrecht Journal of International and European Law* 31, no. 80 (2015): 131.

[11] [2010] IEHC 221. For background see T.J. McIntyre, "Data Retention in Ireland: Privacy, Policy and Proportionality," *Computer Law & Security Report* 24, no. 4 (2008): 326.

[12] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others.*

[13] [2014] IEHC 310.

[14] Henry Farrell, "The Case That Might Cripple Facebook," *The Washington Post*, June 20, 2014, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/06/20/the-case-that-might-cripple-facebook/.

[15] Case C-362/14.

[16] For details of the hearing before the Grand Chamber and the possible impact of the case see Daniel Cooper and Philippe Bradley-Schmieg, "CJEU Hears Oral Arguments in Pivotal EU-US Safe Harbor Case," *The National Law Review*, March 30, 2015, http://www.natlawreview.com/article/cjeu-hears-oral-arguments-pivotal-eu-us-safe-harbor-case-court-justice-european-unio; Derek Scally, "Austrian Student's 'Case of Great Principle,'" *The Irish Times*, March 25, 2015, http://www.irishtimes.com/business/technology/austrian-student-s-case-of-great-principle-1.2151953; Derek Scally, "European Court Hearings Expose Lack of Privacy Safeguards for Our Data," *The Irish Times*, March 27, 2015, http://www.irishtimes.com/opinion/european-court-hearings-expose-lack-of-privacy-safeguards-for-our-data-1.2154885; Samuel Gibbs, "Leave Facebook If You Don't Want to Be Spied On, Warns EU," *The Guardian*, March 26, 2015, http://www.theguardian.com/technology/2015/mar/26/leave-facebook-snooped-on-warns-eu-safe-harbour-privacy-us.

[17] *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation* 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

which has suggested that the warrant contravenes international law by demanding data in a way which does not meet EU data protection standards.[18] In a rare move, the Irish government has intervened by filing an *amicus curiae* brief which argues that the warrant presents issues for Irish sovereignty and that the matter should be dealt with under the existing Mutual Legal Assistance Treaty ("MLAT") between Ireland and the United States.[19]

How and why has this transition – from a largely domestic concept of privacy to one with a significant international dimension – taken place? This chapter surveys the law and suggests that the historically low impact of international information privacy norms in the Irish legal system can be explained by a combination of factors including a strong constitutional privacy right and limited use of surveillance evidence in criminal prosecutions. It goes on to discuss recent developments – in particular changing policing practices, the developing importance of the CFR in privacy cases, and the growth of the internet industry in Ireland – and identifies these as creating countervailing pressures which are increasingly forcing domestic law and policymakers to engage with international privacy standards.

Privacy in the Irish courts: from domestic to international standards

The attitude of the Irish courts to the ECHR has evolved significantly in recent years. Egan[20] has described an initial resistance and even hostility to ECtHR jurisprudence – with the courts instead preferring to address rights issues based solely on domestic law and the Constitution. From the mid to late 1990s onwards, however, there has been a growing receptiveness to ECHR arguments – to the point where the courts have on occasion been willing to consider ECtHR case law even in matters of constitutional interpretation.[21] This trend has strengthened following the incorporation of the ECHR into Irish law by the 2003 Act, mitigating previous concerns that the use of ECHR norms would undermine the dualist nature of the Irish legal system. As de Burca puts it in a more recent assessment, the Irish courts overall now regard the ECHR as an "additional resource for enhancing or strengthening certain rights, bringing other neglected or missing protections into Irish cases, informing the interpretation of the Constitution, and, in some cases, pointing out the incompatibilities of domestic legislation".[22]

---

[18] Richard Waters, "EU Rebukes US over Microsoft Email in First Test of Privacy," *Irish Times*, July 1, 2014, http://www.irishtimes.com/business/sectors/technology/eu-rebukes-us-over-microsoft-email-in-first-test-of-privacy-1.1850750.

[19] See generally Dan Svantesson and Felicity Gerry, "Access to Extraterritorial Evidence: The Microsoft Cloud Case and beyond," *Computer Law & Security Review*, 2015, doi:10.1016/j.clsr.2015.05.007.

[20] Suzanne Egan, "The European Convention on Human Rights Act 2003: A Missed Opportunity for Domestic Human Rights Litigation," *Dublin University Law Journal* 25 (2003): 230.

[21] See also Cian C. Murphy, "Ireland & the UK in the European Union and European Convention on Human Rights: A Tale of Two Island Legal Systems?," in *The National Judicial Treatment of the ECHR and EU Laws. A Comparative Constitutional Perspective* (Groningen: Europa Law Publishing, 2010), http://papers.ssrn.com/abstract=1701953.

[22] Gráinne de Burca, "The Domestic Impact of the EU Charter of Fundamental Rights," *The Irish Jurist*, 2013, 49. Though compare O'Mahony's argument that there is still a degree of judicial hostility and underuse of the ECHR in Irish courts: Barry Roche, "European Court of Human Rights Underused in Irish Law - Lecturer," *The Irish Times*, January 28, 2015, http://www.irishtimes.com/news/ireland/irish-news/european-court-of-human-rights-underused-in-irish-law-lecturer-1.2083248.

This is particularly important in the sphere of privacy, where Irish law lacks explicit constitutional protection. While a number of cases have found an unenumerated right to privacy in the Constitution, the scope of that right is still considerably narrower than that of Article 8 ECHR.[23] Consequently cases such as *Foy v. An t-Ard Chláraitheoir*[24] and *Donegan v. Dublin City Council*[25] have been important in their willingness to apply Article 8 standards against domestic measures. *Donegan* illustrates the divergence in standards particularly well by granting a declaration of incompatibility against a statutory provision allowing for a housing authority tenancy to be terminated without fair procedures – a measure which, prior to 2003, had stood up to constitutional challenge in a number of cases.[26]

Despite this general judicial receptiveness, when we examine the information privacy case law we find that the ECtHR jurisprudence on Article 8 has had surprisingly little influence.

In some important cases – such as the judgments in *Gray v. Minister for Justice*[27] on garda leaking of information and *DPP v. Boyce*[28] on the collection of DNA evidence – there is simply no reference to the ECHR. In others Article 8 is mentioned only to be dismissed as irrelevant or unnecessary. In *White v. Morris*[29], for example, the High Court considered whether a witness before a tribunal of inquiry was entitled to have medical evidence heard in private. In deciding that he was not, Finnegan J. held that the matter could be determined based solely on the domestic case law, stating that "I do not see that these provisions [of Article 8] add anything to the constitutional right to privacy and in particular the Convention, as does the Constitution, requires a balancing of interests". Similarly, in *Herrity v. Associated Newspapers*[30] the High Court held that it was not necessary to consider Article 8 in determining whether a newspaper had breached the constitutional rights of the plaintiff by publishing details of an illegally intercepted telephone conversation, accepting without any discussion that Irish law on this point was in compliance with the ECHR.

While those cases were unusual in excluding any consideration of Article 8, even those cases which did address it tended to do so only in a cursory way as an appendix to more detailed consideration of the constitutional right. The leading decision on undercover media filming – *Cogley and Aherne v. RTE*[31] – mentions the ECHR right to privacy only in passing and places greater reliance on authority from New Zealand. Similarly, the decision in *DPP v Colm Murphy*[32] on the collection and use of telephone records in criminal proceedings gives only two paragraphs to considering

[23] For a recent analysis see Denis Kelleher, *Privacy and Data Protection Law in Ireland*, 2nd ed. (Haywards Heath: Bloomsbury Professional, 2015), chap. 2 and 3.
[24] [2007] IEHC 470.
[25] [2008] IEHC 288.
[26] See *State (O'Rourke) v. Kelly* [1983] IR 58; *Dublin Corporation v. Hamilton* [1999] 2 IR 486; *Dublin City Council v. Fennell* [2005] 1 IR 604.
[27] [2007] IEHC 52.
[28] [2008] IESC 62.
[29] [2007] IEHC 107.
[30] [2008] IEHC 249.
[31] [2005] IEHC 181.
[32] [2005] IE CCA 1.

whether this practice meets the standards set out in *Malone v. United Kingdom.*[33] It was only in 2010 that the first judgments began to appear which engaged with Article 8 in any detail.[34]

Why did these cases make little use of Article 8 at a time when the Irish courts were otherwise increasingly having regard to the ECHR? There are a number of possible answers ranging from the priorities of civil liberties groups, to the tactical choices of litigants to the receptiveness of individual judges. The main reason, however, appears to be the strength of the constitutional right to information privacy. Unlike England, where the courts struggled to identify a legal basis for privacy and had to rely on Article 8 to develop the doctrine of breach of confidence into a wider action of misuse of private information, the decision in *Kennedy and Arnold v. Ireland*[35] established early on that there was a freestanding cause of action for breach of privacy. In addition, the Irish courts have long accepted that constitutional rights can attract remedies both against the State and against private parties[36] – without any need to grapple with the difficult question of indirect horizontal effect of ECHR rights.[37] The comment of Finnegan J. in *White v. Morris*[38] that Article 8 does not "add anything to the constitutional right to privacy" reflected the strength of the domestic right and highlighted a judicial preference in these cases to reach a decision on purely domestic grounds where possible.

This approach was unproblematic so long as domestic law and international norms led to the same result. It has, however, led to some decisions which are inconsistent with Article 8. The most striking example is *Atherton v. DPP*[39] on the admissibility of covert video evidence. In this case the accused was charged with damaging his neighbour's hedge. The neighbour – apparently on the advice of a garda – set up a video camera in an upstairs window which recorded a view of the hedge but also looked into the accused's driveway, garden, front door and front windows. The accused argued that the resulting video footage had been obtained unlawfully and in breach of his constitutional rights – relying extensively on Article 8 case law. Peart J., however, did not address that case law at all but instead focused solely on the domestic law. He held that there was no invasion of the right to privacy where "the front of the accused's house is something which is visible from the public road—perhaps only with the use of a ladder, but nonetheless visible". He went on to say that while "a different view might easily be taken if the act of setting up the camera in the required position involved a trespass upon the property of the person to be observed" this was not such a case. Finally, Peart J. held that "there is no meaningful distinction between the evidence of what was happening to the hedge in the garden opposite that house being given in the form of video footage, and that very same evidence being given by the owner of the house opposite if he… was standing at the same window as the camera was set up at and observing himself what was happening".

---

[33] Application no. 8691/79, judgment of 2 August 1984.
[34] See in particular *Digital Rights Ireland v. Minister for Communications* [2010] IEHC 221, *Hickey v. Sunday Newspapers* [2010] IEHC 349, *Murray v. Newsgroup Newspapers* [2010] IEHC 248 and *HSE v. A and B* [2010] IEHC 360.
[35] [1987] IR 1.
[36] *Meskell v. CIE* [1973] IR 121; *Herrity v. Associated Newspapers* [2008] IEHC 249.
[37] Daithí Mac Síthigh, "Beyond Breach of Confidence: An Irish Eye on English and Scottish Privacy Law," *Juridical Review* 2014 (2014): 27.
[38] [2007] IEHC 107.
[39] [2005] IEHC 429.

From an Article 8 perspective, however, the judgment in *Atherton* is deeply problematic. It relies on the fact that the area was visible from the public road (with the aid of a ladder!) and from the facing houses to deny that any privacy interest existed. It also appears to introduce a "trespass doctrine" reminiscent of since discredited US authority.[40] But this approach is inconsistent with the decision of the ECtHR in *Peck v. the United Kingdom*[41] which makes it clear that privacy rights can subsist even in respect of CCTV footage of public areas. *Peck* confirms that privacy under Article 8 is a context-specific concept, where the fact that an event takes place in a public place is just one element in the overall assessment of whether there has been an interference with private life – by relying instead on a simplistic public/private divide *Atherton* clashes with established ECtHR doctrine.[42] It is somewhat ironic that in this way the strong domestic privacy right articulated in *Kennedy v. Ireland*[43] can effectively crowd out consideration of the ECHR and contribute to a weakening of privacy rights overall.

Applying privacy standards to surveillance

Another reason for the relatively limited impact of Article 8 in the Irish legal system is structural: state surveillance has predominantly been used for intelligence rather than prosecution purposes, minimising disclosure of surveillance tactics and possible judicial scrutiny. In relation to intercepted phone calls there is a settled policy on the part of police and prosecutors to use these for intelligence only[44] even though there is no statutory prohibition on the use of intercept evidence in criminal prosecutions.[45] Until recently, evidence obtained by bugging of buildings or cars was treated in the same way.[46] In 2007, then Minister for Justice Brian Lenihan explained this on the basis that "by using bugged and intercepted conversations as evidence in prosecutions, the force ran the risk of alerting criminals to Garda investigative techniques".[47]

This restriction had an important side effect – it limited the opportunities for the courts to assess the fundamental rights compliance of surveillance. As Heffernan has noted, the law of evidence plays an important part in police governance in Ireland.[48] When defendants challenge the admissibility of evidence they enable the courts to review the legality of police behaviour and help to hold gardaí accountable for failure to abide by the law. Because garda surveillance material has generally not been used

[40] See *Olmstead v. United States*, 277 US 438 (1928). The requirement of trespass for an action to constitute a Fourth Amendment search was overturned in *Katz v. United States*, 389 US 347 (1967).
[41] Application no. 44647/98, judgment of 28 January 2003.
[42] Other problems include the way in which *Atherton* treats video recording and eye witness testimony as equivalent, overlooking the additional privacy issues presented by the continuous and permanent nature of recording. For further discussion see Eoin Carolan, "Stars of Citizen CCTV: Video Surveillance and the Right to Privacy in Public Places," *Dublin University Law Journal*, 2006, 326.
[43] [1987] IR 1.
[44] JUSTICE, *Intercept Evidence: Lifting the Ban* (London, 2006), 56–57, http://www.justice.org.uk/data/files/resources/40/Intercept-Evidence-1-October-2006.pdf.
[45] In *DPP v Colm Murphy* [2005] IECCA 1 the Court of Criminal Appeal stated *obiter* that intercept evidence is admissible.
[46] Paul Golden, "Technology against Crime," *Garda Review* 36, no. 7 (2008).
[47] Conor Lally, "New Surveillance Powers Considered," *The Irish Times*, November 2, 2007, http://www.irishtimes.com/news/new-surveillance-powers-considered-1.978171.
[48] Liz Heffernan, "Police Accountability and the Irish Law of Evidence," *Crime, Law and Social Change* 55, no. 2–3 (April 2011): 185.

in prosecutions there has been little insight into its operation and few opportunities for the courts to consider whether surveillance meets the requirements of Article 8 ECHR.[49]

This lack of scrutiny also meant that the State was able to persist with largely unregulated surveillance practices despite the fact that they did not meet ECHR standards. Article 8 requires that interferences with the right to private life must be "in accordance with the law". Broadly speaking, this principle of legality requires three conditions to be met in respect of surveillance. The first is that there should be a legal basis for the interference. The second is legal foreseeability, which requires that "the law must indicate the scope of [the discretion to order surveillance] conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".[50] The third condition is that the law must provide "adequate and effective guarantees against abuse" to counter the increased risks resulting from the secret nature of the surveillance. This involves a contextual analysis which looks at the invasiveness of the particular surveillance system and the controls which serve to restrain it. In particular, it requires that there should be a supervisory body which is "independent of the authorities carrying out the surveillance", "objective" and "vested with sufficient powers and competence to exercise an effective and continuous control".[51]

Historically, however, the State has used surveillance without any explicit legal basis, with regulation introduced reluctantly and belatedly when some scandal or outside pressure pushed the issue onto the agenda.[52] Legislation on the interception of communications was adopted in 1993 only after Taoiseach Charles Haughey was forced from office for bugging journalists' telephones – and has not been updated since then, despite fundamental technological changes in the meantime.[53] Legislation on data retention was first passed in 2005, largely because the Data Protection Commissioner threatened legal action if the practice was not put on a statutory basis.[54] Legislation on covert surveillance came about only in 2009 following the public pressure caused by two high profile gang murders in Limerick.[55] There are, even now,

[49] The one exception is data retention, where this point was addressed – albeit very briefly – in *DPP v Colm Murphy* [2005] IECCA 1.

[50] *Weber and Saravia v. Germany*, application no. 54934/00, judgment of 29 June 2006, para. 94. Para. 95 of that decision goes on to summarise the necessary safeguards in the context of telephone tapping: "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

[51] *Klass v. Germany*, application no. 5029/71, judgment of 6 September 1978, para. 56.

[52] For example, the Law Reform described visual surveillance as taking place in a "legal vacuum": *Consultation Paper on Privacy: Surveillance and the Interception of Communications* (Dublin, 1996), 221, http://www.lawreform.ie/publications/data/lrc91/lrc_91.html.

[53] Maurice Collins, "Telephone Tapping and the Law in Ireland," *Irish Criminal Law Journal* 3 (1993): 31.

[54] McIntyre, "Data Retention in Ireland."

[55] Peter Kirwan, "Covert Surveillance - The Case for Legislative Authority," *Garda Communique*, November 2008; Paul Anthony McDermott, "Undercover Investigations & Human Rights" (9th Annual National Prosecutors' Conference, Dublin, May 24, 2008), http://www.dppireland.ie/filestore/documents/PAPER_-_Paul_Anthony_McDermott_BL.pdf; Alisdair

no statutory controls on the use of informants or undercover police agents.[56] Against this background it is not surprising that the ill-fated Privacy Bill 2006, which proposed to create a far-reaching tort of "violation of privacy", specifically excluded state surveillance from its scope and would have provided a blanket immunity for "any act done by a public servant… acting in the course of his or her duties".[57]

As a result, there have been few opportunities for either the legislature or the courts to examine the rights issues presented by state surveillance. This is, however, now beginning to change. Both the *Digital Rights Ireland* and *Schrems* cases have resulted in important statements of legal principle and in addition the Criminal Justice (Surveillance) Act 2009 has put several aspects of state surveillance under greater scrutiny. The 2009 Act did not introduce garda bugging of premises and planting of GPS tracking devices on vehicles; instead, it legislated for existing practices. The aim was to provide the basis to allow evidence to be used in prosecutions, not merely for intelligence purposes – making a deliberate trade-off between secrecy and the ability to obtain convictions.[58] In doing so, the 2009 Act introduced several new aspects into Irish surveillance law. For the first time there is a requirement of judicial authorisation before surveillance can be carried out[59]; there is a prohibition on granting an authorisation where "the surveillance is likely to relate primarily to communications protected by privilege"[60]; and there is provision for notification after the fact of those affected by surveillance.[61]

These safeguards seem to have varying origins – in part reflecting the constitutional guarantee of the inviolability of the dwelling, in part ECtHR jurisprudence under Article 8 – but collectively they represent a significant step forward compared to previous practice.[62] They also highlight the inadequacy of the law in other areas, especially the interception of telephone calls. The 1993 interception legislation[63] was

---

A. Gillespie, "Covert Surveillance, Human Rights and the Law," *Irish Criminal Law Journal* 19, no. 3 (2009): 71; T.J. McIntyre, "Operation Observation Comes to Our Shores," *Sunday Business Post*, April 19, 2009, http://archives.tcm.ie/businesspost/2009/04/19/story41144.asp.

[56] 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, 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, 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, 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.

[57] Section 5(1)(c)(i).

[58] Marie O'Halloran, "Garda 'Railroaded' into Accepting Covert Legislation," *The Irish Times*, April 30, 2009, http://www.irishtimes.com/newspaper/ireland/2009/0430/1224245682910.html.

[59] Section 5. However approval for surveillance can be granted internally in cases of urgency under section 7, and the planting of tracking devices also requires only internal approval under section 8.

[60] Section 5(4).

[61] Section 10(3) provides that the Minister may make regulations dealing with notification. However, no such regulations have been made – effectively negating the provision.

[62] Though they are far from ideal. In particular there is no good reason why judicial authorisation should not be required in all cases. For criticism see Denis Kennedy and Yukun Zong, "The Privacy Protection in Electronic Surveillance: A Comparative Research Project between Irish and German Criminal Justice," *Freilaw – Freiburg Law Students Journal* 3 (2014): 28; Gillespie, "Covert Surveillance, Human Rights and the Law."

[63] The Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

drafted to take ECHR standards of the time into account, but has not been updated to take account of significant developments since then. The 2009 Act reflects the subsequent jurisprudence of the ECtHR which now requires greater protections to be put in place in respect of matters such as judicial authorisation and oversight[64], protection of privileged lawyer/client communications[65], and notifying individuals that they have been the subject of surveillance.[66] It therefore provides an important comparator which civil liberties advocates can use to ask why similar protections do not apply to other forms of surveillance also.

The 2009 Act has already resulted in one successful challenge to the admissibility of surveillance evidence – in *Sunny Idah v. DPP*[67] recordings of face to face meetings between the appellant and undercover gardaí were found to be inadmissible where such recordings had not been authorised in accordance with the 2009 Act and where there was no element of urgency to justify the failure to seek an authorisation. Significantly, that case relied on ECtHR jurisprudence[68] in determining the extent of the right to privacy in the context of covert surveillance, and it is likely that further cases under the 2009 Act will result in increased scrutiny of surveillance practices against international standards.

The growing importance of the Charter of Fundamental Rights

In an Irish context the most important sources of international human rights law have historically been the International Bill of Human Rights and the ECHR. In the case of privacy, however, the EU Charter of Fundamental Rights is now equally – if not more – important. The CFR has only been binding on the EU and Member States since the entry into force of the Lisbon Treaty on 1 December 2009. Nevertheless, during that short period it has had a huge impact on internet privacy.[69] In addition to the *Digital Rights Ireland* and *Schrems* cases on state surveillance the CJEU has also relied on the CFR in *Google Spain*[70] to develop the so-called "right to be forgotten" as against search engines.[71]

Why is the CFR so significant for privacy law? A key reason is that it goes considerably further than other human rights instruments by recognising "protection of personal data" as a fundamental right parallel to but distinct from the right to

[64] See T.J. McIntyre, "Judicial Oversight of Surveillance: An Irish Perspective," in *Judges as Guardians of Constitutionalism and Human Rights*, ed. Martin Scheinin, Helle Krunke, and Marina Aksenova (Cheltenham: Edward Elgar, forthcoming).
[65] See e.g. *Kopp v. Switzerland*, application 23224/94, judgment of 25 March 1998.
[66] 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), http://ejlt.org/article/view/155.
[67] [2014] IECCA 3.
[68] *Lüdi v. Switzerland*, application no. 12433/86, judgment of 15 June 1992.
[69] Gabriela Zanfir, "How CJEU's 'Privacy Spring' Construed the Human Rights Shield in the Digital Age," in *European Judicial Systems as a Challenge for Democracy*, ed. Elzbieta Kuzelewska et al. (Cambridge: Intersentia, 2015).
[70] Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.
[71] Or more accurately, the right to have certain information removed from search results appearing in response to a person's name. See e.g. Orla Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez," *The Modern Law Review* 78, no. 3 (2015): 522.

privacy.[72] While Article 7 CFR simply mirrors the ECHR by providing that "[e]veryone has the right to respect for his or her private and family life, home and communications", Article 8 CFR adds a new right which has no counterpart under the ECHR:

> Article 8
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

The CFR therefore elevates data protection from a mere statutory right to one which is on a par with other fundamental rights. It also creates new obligations – such as the right of access to data and rectification of data – which are not recognised as aspects of the right to privacy under more traditional human rights instruments. As a result, the CFR is significantly more protective of privacy than the ECHR.[73] This can be seen when we consider the judgment of the CJEU in *Digital Rights Ireland* finding that the Data Retention Directive was disproportionate under Articles 7 and 8 of the Charter. While the CJEU found fault with many aspects of the Directive, one of the most significant flaws it identified was the lack of independent judicial approval before communications data could be accessed[74] – something prior ECtHR decisions had regarded as unproblematic.[75]

The scope of the CFR is also important, as it will cover many privacy issues which might at first glance seem to be purely matters of domestic law. While the CFR does not generally apply to member states' own actions, it will do so when member states are "implementing" EU law.[76] As interpreted by the CJEU in *Fransson*[77] and *Pfleger*,[78] this will include "all situations governed by" or "within the scope of" EU law, including derogations from EU law.[79] In practice, this extends the CFR to cover many forms of national surveillance, as these will usually involve member states relying on either the derogations in the e-Privacy Directive[80] (to intercept communications or capture communications data) or else the derogations in the Data

[72] The difference between the two rights is discussed in Juliane Kokott and Christoph Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law* 3, no. 4 (November 1, 2013): 222–28, doi:10.1093/idpl/ipt017.
[73] See e.g. the judgment of the English High Court in *R (Davis) v. Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) holding at para. 80 that Article 8 CFR "clearly goes further, is more specific, and has no counterpart in the ECHR" and therefore should not be interpreted downward to accord with ECtHR decisions.
[74] Para. 62.
[75] Compare *PG and JH v. United Kingdom*, application no. 44787/98, judgment of 25 September 2001.
[76] Article 51. See generally Xavier Groussot, Laurent Pech, and Gunnar Thor Petursson, "The Scope of Application of Fundamental Rights on Member States' Action: In Search of Certainty in EU Adjudication," Eric Stein Working Papers (Prague: Czech Society for European and Comparative Law, 2011), http://www.ericsteinpapers.cz/images/doc/eswp-2011-01-groussot.pdf.
[77] Case C-617/10, *Åklagaren v. Hans Åkerberg Fransson*.
[78] Case C-390/12, *Pfleger and others*.
[79] *Pfleger*, paras. 30-37.
[80] Directive 2002/58/EC.

Protection Directive[81] (to collect and process personal data).[82] This has been confirmed by recent cases in the United Kingdom and the Netherlands where national courts have found domestic data retention laws to be within the scope of the CFR and therefore, applying *Digital Rights Ireland*, in violation of Articles 7 and 8.[83]

There are also practical advantages to the recognition of privacy and data protection in the CFR which will make it significantly easier for civil liberties groups to assert these rights in the Irish legal system. As EU rights, these now provide litigants with the strategic and tactical advantages of other EU principles such as direct effect, supremacy and the requirement that national law must provide adequate and effective remedies. For example, in the domestic proceedings in the *Digital Rights Ireland* case the High Court accepted that restrictive national rules on standing and security for costs had to be relaxed where their enforcement would frustrate the enforcement of Charter rights, and Digital Rights Ireland was allowed to proceed on the basis of an *action popularis*.[84] Similarly, in *Schrems v. Data Protection Commissioner* the High Court granted Ireland's first protective costs order to the plaintiff.[85] In addition, judgments of the CJEU are self-executing while an applicant may wait some time for a decision of the ECtHR to be addressed in national law – making a reference to Luxembourg rather than an application to Strasbourg a much more attractive option for the enforcement of fundamental rights.[86]

Ireland as an internet hub

Attractive corporation tax rates have made Dublin a hub for the European headquarters of major multinational firms such as Google, Microsoft, Facebook, LinkedIn, Twitter and Yahoo.[87] Almost all these firms hold extensive user data in Ireland and many have designated their Irish subsidiary as the data controller for all users outside the United States.[88] Because of this, Irish privacy law is no longer merely a domestic issue – it now directly affects the rights of hundreds of millions of internet users throughout Europe and further afield.

---

[81] Directive 95/46/EC.

[82] Where surveillance is purely a matter of national security then it is in principle outside EU competence and the CFR will not apply. However surveillance measures which serve a mixed national security and criminal law purpose would not meet this test.

[83] *R (Davis) v. Secretary of State for the Home Department* [2015] EWHC 2092 (Admin); Wendy Zeldin, "Netherlands: Court Strikes Down Data Retention Law," web page, *Library of Congress Global Legal Monitor*, (March 23, 2015), http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404345_text.

[84] *Digital Rights Ireland Ltd v Minister for Communication* [2010] IEHC 221.

[85] "Update on Ireland's First Protective Costs Order – Europe v. Facebook.org," *Public Interest Law Alliance Bulletin*, July 30, 2014, http://www.pila.ie/bulletin/2014/july-2014/30-july/update-on-ireland-s-first-protective-costs-order-europe-v-facebook-org/.

[86] There is also a cost issue – while an application to the ECtHR requires that domestic remedies have been exhausted, a preliminary reference to the CJEU can be sought at a much earlier stage in the proceedings thereby reducing the financial burden of the case.

[87] Mark Scott, "Ireland Vies to Remain Silicon Valley's Low-Tax Home Away From Home," *New York Times*, November 9, 2014, http://bits.blogs.nytimes.com/2014/11/09/ireland-still-silicon-valleys-low-tax-home-away-from-home/.

[88] See e.g. Facebook, "Data Policy," January 30, 2015, https://www.facebook.com/policy.php; Twitter, "Privacy Policy," May 18, 2015, https://twitter.com/privacy; LinkedIn, "Privacy Policy," October 23, 2014, https://www.linkedin.com/legal/privacy-policy.

This has already resulted in uncomfortable international scrutiny. Max Schrems, the Austrian privacy advocate who established the *Europe v. Facebook* campaign to challenge Facebook's handling of personal data, has been a leading critic. Dissatisfied with the response of the Irish Data Protection Commissioner ("DPC") to his complaints, he has described the Irish regulatory system as being deliberately lax and under-resourced in order to encourage internet firms to locate here.[89] While that portrayal is a little unfair – it attributes the undeniable government underfunding of data protection to a cunning plan rather than simple neglect – it has nevertheless achieved traction throughout Europe.[90] As a result it has forced a significant response aimed at shoring up Ireland's reputation: since 2014 funding for the DPC's office has been doubled, a Minister of State appointed with special responsibility for data protection and a consultative Data Forum established to provide for greater stakeholder input into data protection policy generally.[91]

So long as Ireland hosts a significant portion of the internet industry this spotlight will continue to shine and at least three sets of international stakeholders can be expected to keep a close eye on Irish law.

First, privacy campaigners. The litigation in *Schrems v. Data Protection Commissioner*[92] highlights the fact that the presence of internet giants already makes Ireland a venue for litigation challenging use of our data. This will be even more the case once the proposed EU General Data Protection Regulation ("GDPR") is adopted. A key aim of the GDPR is to ease the regulatory burden on data controllers by providing a "one stop shop" mechanism for data protection oversight.[93] As things stand, multinational businesses in Europe must deal with data protection authorities in each country where they operate. Under the proposed one stop shop system, in important cross-border cases a business will primarily be regulated by a single data protection authority in the country where it has its "main establishment".[94] This will make the Irish Data Protection Commissioner the lead regulator for much of the internet industry, significantly increasing the number of complaints being dealt with under Irish law.

[89] Derek Scally, "Ireland: Prisoner of Big Tech?," *The Irish Times*, May 3, 2014, http://www.irishtimes.com/news/technology/ireland-prisoner-of-big-tech-1.1781833.
[90] Karlin Lillington, "Strong Data Protection Laws Better for EU than Sniping," *The Irish Times*, April 23, 2015, http://www.irishtimes.com/business/technology/strong-data-protection-laws-better-for-eu-than-sniping-1.2185370.
[91] Aine McMahon, "Data Protection Gets Funding Doubled," *Irish Times*, December 18, 2014, http://www.irishtimes.com/news/politics/data-protection-gets-funding-doubled-1.2043073; Elaine Edwards, "Forum to Discuss Use of Personal Data in Digital Economy," *The Irish Times*, April 30, 2015, http://www.irishtimes.com/news/politics/forum-to-discuss-use-of-personal-data-in-digital-economy-1.2195795.
[92] [2014] IEHC 310.
[93] For background see Rosemary Jay, "Data Protection: Making the 'One Stop Shop' Work," *Society for Computers and Law*, November 3, 2014, http://www.scl.org/site.aspx?i=ed39323.
[94] For discussion of the current draft see "Bureaucracy Will Prevail in 'One Stop Shop' Data Protection Regime, UK and Ireland Warn," *Out-Law.com*, March 13, 2015, http://www.out-law.com/en/articles/2015/march/bureaucracy-will-prevail-in-one-stop-shop-data-protection-regime-uk-and-ireland-warn/.

Second is the internet industry itself. Following the Snowden disclosures, customers of internet firms have become increasingly privacy conscious.[95] Customer trust now depends on the jurisdiction in which information is stored – and firms headquartered in Ireland have expressed concern that their commercial position could be harmed by a perception that Irish law is lax. In a confidential November 2014 meeting between senior executives in Google and the Minister for Finance, Michael Noonan, Google is reported as stressing that "data privacy and surveillance by Government is an important issue … the Governments' policies for requesting information from Internet companies needs to be clear and transparent" and "the strength of a country's competent authority for data privacy [is] now as important an issue for a country's competitive edge as their competent authority for taxation".[96] This corporate lobbying for stronger privacy rights is particularly significant: experience has shown that Irish governments are receptive to economic arguments in circumstances where fundamental rights arguments fall on deaf ears.

Internet firms are also bringing more attention to surveillance practices through their adoption of transparency reports. Pioneered by Google and since adopted by most of its peers, these reports aim to promote customer trust by describing the legal basis for disclosure of user information and providing statistics on the number of government requests for user data.[97] For each jurisdiction they will typically state how many official requests were received, how many users were affected and what percentage of the requests resulted in data being disclosed. These reports have helped to fill in some of the blanks in the otherwise secretive Irish system, and by highlighting the uncertain legal basis for internet surveillance have already provoked considerable media attention and helped to make the case for rights-based reform.[98]

Third, law enforcement and national security agencies from other jurisdictions are increasingly seeking to access information held here and those states are already pushing for changes to facilitate this.[99] This trend was predicted by Swire, who in

---

[95] Ben Young, "Data Privacy Isn't Political — It's Personal," *Gigaom Research*, July 27, 2014, https://gigaom.com/2014/07/27/data-privacy-isnt-political-its-personal/.

[96] Sarah McCabe, "Data Privacy Is as Important as Tax, Google Exec Warns Noonan," *Irish Independent*, April 12, 2015, http://www.independent.ie/business/irish/data-privacy-is-as-important-as-tax-google-exec-warns-noonan-31134213.html; Department of Finance, "Summary Note of Meeting with John Herlihy and Urs Hozle of Google," November 5, 2014, https://www.digitalrights.ie/dri/wp-content/uploads/2015/05/Note-of-meeting-between-Google-and-Noonan.pdf.pdf (released under the Freedom of Information Act).

[97] Joshua Kopstein, "Silicon Valley's Surveillance Cure-All: Transparency," *The New Yorker*, October 1, 2013, http://www.newyorker.com/tech/elements/silicon-valleys-surveillance-cure-all-transparency.

[98] See e.g. "Gardaí Sought Access to Hundreds of Private Emails," *Irish Examiner*, March 22, 2013, http://www.irishexaminer.com/ireland/gardai-sought-access-to-hundreds-of-private-emails-226189.html; Jack Horgan-Jones, "Only One Country Refused to Allow Vodafone Publish Spying data…Ireland," *TheJournal.ie*, June 6, 2014, http://www.thejournal.ie/vodafone-government-refusals-makey-uppy-law-1502972-Jun2014/; Conor Pope, "Vodafone Report Sparks Interception Law Concerns," *The Irish Times*, June 7, 2014, http://www.irishtimes.com/news/consumer/vodafone-report-sparks-interception-law-concerns-1.1823901; Dan MacGuill, "State Surveillance: How Gardaí and Others Can Secretly Monitor You," *TheJournal.ie*, May 17, 2015, http://www.thejournal.ie/state-surveillance-ireland-gardai-wiretapping-email-monitoring-gardai-2099537-May2015/; Dan MacGuill, "State Surveillance: What the Government and Gardaí Don't Want You to Know," *TheJournal.ie*, May 17, 2015, http://www.thejournal.ie/ireland-state-surveillance-wiretapping-gardai-crime-transparency-2105584-May2015/.

[99] See e.g. Nick Hopkins, "Theresa May Warns Yahoo That Its Move to Dublin Is a Security Worry," *The Guardian*, March 20, 2014, http://www.theguardian.com/technology/2014/mar/20/theresa-may-

2012 observed that the move away from conventional telephony and towards the use of encrypted internet services creates significant problems for traditional real time wiretapping.[100] As a result, governments are increasingly reliant on accessing stored communications in cloud services such as Hotmail. As Swire puts it, this creates a division between states which are information "haves" – where firms are based who can be compelled to provide information under domestic law – and information "have nots", who will be dependent on cooperation from the "have" jurisdictions using MLAT requests.[101] (Or, more controversially, by asserting that their laws have extraterritorial effect.[102]) As an information "have", Ireland is set to be a battleground for future disputes around state access to personal data – again, forcing the courts and policy makers to engage with international privacy norms to a greater extent.

Conclusion

This chapter has illustrated the fact that the reception of international human rights norms into national law is a contingent process, even in a democracy with established civil society groups, statutory human rights institutions and increasing judicial and practitioner awareness of the international rights regimes. It has argued that in a perverse way the strong privacy right articulated in *Kennedy and Arnold v. Ireland*[103] has held back the development of information privacy law, as has the effective inability to challenge surveillance practices which are used for intelligence purposes rather than to gather evidence. It has also noted more recent changes in the wider legal and commercial environment which are increasingly forcing international privacy norms onto the domestic agenda, particularly as newer civil society groups such as Europe v. Facebook and Digital Rights Ireland have focused on litigation as a tool to promote internet privacy.

Ideally, the growth of the "information economy" in Ireland would have prompted a wide debate regarding the way in which Irish law protects privacy. To date, however, the involvement of policy makers and the legal system with international privacy norms has been largely *ad hoc* and reactive, and it would be unfortunate if this pattern were to continue. There is a pressing need for a wider assessment of Irish privacy law against international standards, particularly in the area of state surveillance of communications. While cases such as *Schrems* and *Digital Rights Ireland* have served to highlight international rights issues, litigation remains an expensive and slow mechanism which at worst can be a distraction from other approaches towards enforcing international standards.[104] That said, we can expect litigation in this area to increase unless Irish governments become more willing to proactively engage with international human rights standards.

---

yahoo-dublin-security-worry; David Anderson, "A Question of Trust – Report of the Investigatory Powers Review" (London: Independent Reviewer of Terrorism Legislation, June 2015), para. 11.26, https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/.

[100] Peter Swire, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," *International Data Privacy Law* 2, no. 4 (November 1, 2012): 200.

[101] Ibid., 206.

[102] Svantesson and Gerry, "Access to Extraterritorial Evidence."

[103] [1987] IR 1.

[104] See e.g. Beth A Simmons, *Mobilizing for Human Rights International Law in Domestic Politics* (Cambridge: Cambridge University Press, 2009), 129–135.

Further reading

Carolan, Eoin. “Stars of Citizen CCTV: Video Surveillance and the Right to Privacy in Public Places.” *Dublin University Law Journal*, 2006, 326.

Gillespie, Alisdair A. “Covert Surveillance, Human Rights and the Law.” *Irish Criminal Law Journal* 19, no. 3 (2009): 71.

Law Reform Commission. *Report on Privacy Surveillance and the Interception of Communications*. Dublin, 1998.

McIntyre, T.J. “Data Retention in Ireland: Privacy, Policy and Proportionality.” *Computer Law & Security Report* 24, no. 4 (2008): 326.

McIntyre, T.J. “Judicial Oversight of Surveillance: An Irish Perspective.” In *Judges as Guardians of Constitutionalism and Human Rights*, edited by Martin Scheinin, Helle Krunke, and Marina Aksenova. Cheltenham: Edward Elgar, forthcoming.

Murphy, Maria Helen. “The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases.” *Irish Journal of Legal Studies* 3, no. 2 (2013): 65.

Murphy, Maria Helen. “Data Retention in the Aftermath of Digital Rights Ireland and Seitlinger.” *Irish Criminal Law Journal*, no. 4 (2014): 105.

Svantesson, Dan, and Felicity Gerry. “Access to Extraterritorial Evidence: The Microsoft Cloud Case and beyond.” *Computer Law & Security Review*, 2015. doi:10.1016/j.clsr.2015.05.007.