Title	Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective
Authors(s)	McIntyre, T. J.
Publication date	2016-04
Publication information	Scheinin, M., Krunke, H. and Aksenova, M. (eds.). Judges as Guardians of Constitutionalism and Human Rights
Publisher	Edward Elgar
Link to online version	http://www.e-elgar.com/shop/judges-as-guardians-of-constitutionalism-and-human-rights
Item record/more information	http://hdl.handle.net/10197/7363
Publisher's statement	Edward Elgar Publishing is the source and copyright holder of the work, and the article cannot be used for any other purpose elsewhere. The chapter is for private use only.

Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective

Dr. TJ McIntyre, UCD Sutherland School of Law and Digital Rights Ireland

This is a draft chapter that has been accepted for publication by Edward Elgar Publishing in *Judges as Guardians of Constitutionalism and Human Rights,* edited by Martin Scheinin, Helle Krunke, and Marina Aksenova, due to be published in 2016.

1. Introduction

Secret state surveillance has long been regarded as a grave threat to constitutionalism, putting at risk not only individual rights but also the wider democratic process. In the landmark decision in *Klass v. Germany* the European Court of Human Rights (ECtHR) described it as a necessity which nevertheless posed a danger of "undermining or even destroying democracy on the ground of defending it".[1] That decision reflected concerns over technical advances which made surveillance more sophisticated – concerns which are all the more acute following the Edward Snowden revelations of mass surveillance on an unprecedented scale, capturing the communications of all people indiscriminately.[2]

At both national and international levels, human rights law has responded by demanding effective oversight of surveillance by independent institutions – but there is an ongoing debate as to what role the judiciary should play. In *Klass v. Germany* the ECtHR expressed a strong preference for judicial control at the point where surveillance is first ordered and while it is being carried out, stating that "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge".[3] Despite this, the court did not require prior judicial control or even overall judicial supervision, holding instead that other systems could be permissible where the supervisory bodies were "independent of the authorities carrying out the surveillance", "objective" and "vested with sufficient powers and competence to exercise an effective and continuous control".[4]

This compromise position has been challenged as surveillance faces greater scrutiny worldwide, and there are strong arguments that a judicial dimension to oversight is now essential.[5] For example, in a significant June 2014 report on the right to privacy in the digital age the Office of the UN High Commissioner for Human Rights (OHCHR) concluded that "the involvement of all branches of

[1] *Klass v. Germany*, application 5029/71, 6 September 1978, para. 49.

[2] See e.g. Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (June 1, 2014): 121.

[3] *Klass v. Germany*, application 5029/71, 6 September 1978, para. 56.

[4] *Ibid*.

[5] See in particular Electronic Frontier Foundation and Article 19, "Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance," *Necessary and Proportionate*, May 2014, https://en.necessaryandproportionate.org/LegalAnalysis.

government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law". That report warned, however, that judicial involvement should not be viewed as a panacea and noted that in a number of countries "judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping".[6] Instead the OHCHR recommended a mixed model, which would combine administrative, judicial and parliamentary oversight. In the United Kingdom, 2015 saw the publication of two influential reports from the Independent Reviewer of Terrorism Legislation[7] and the Independent Surveillance Review[8], both of which recommended that there should be prior judicial authorisation of all warrants to intercept communications, with some limitations in the case of national security warrants.[9]

This chapter contributes to this discussion by considering in more detail how judicial oversight interacts with communications surveillance. The author is chair of the civil liberties group Digital Rights Ireland (DRI) which was the lead plaintiff in the April 2014 decision of the European Court of Justice invalidating the Data Retention Directive[10] and is currently challenging domestic Irish data retention laws.[11] The chapter reflects this by focusing on Irish, European Convention on Human Rights (ECHR) and European Union (EU) law. It begins by considering the general arguments for judicial oversight and the types of oversight structures which can be used. It then examines the extent to which Irish, ECHR and EU law require judicial oversight in particular circumstances. Next, it takes as a case study the Irish experience of data retention. It concludes with suggestions for improving the effectiveness of judicial involvement in surveillance.

2. Why judicial oversight?

As a preliminary matter we might ask a question which is sometimes overlooked: why is judicial oversight desirable? What is it that makes judges (as distinct from parliamentarians or members of other independent bodies) particularly suitable for this role? In *Klass v. Germany* the Grand Chamber gave a structural justification, stating that:

> "The rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the

[6] Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in a Digital Age," June 30, 2014, 12–13, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[7] David Anderson, "A Question of Trust – Report of the Investigatory Powers Review" (London: Independent Reviewer of Terrorism Legislation, June 2015), https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/.

[8] Independent Surveillance Review, "A Democratic Licence to Operate" (London: Royal United Services Institute, 2015), https://www.rusi.org/downloads/assets/ISR-Report-press.pdf.

[9] Though compare the report of the United Kingdom Intelligence and Security Committee which argues for the retention of authorisation by Ministers: *Privacy and Security: A Modern and Transparent Legal Framework.* (London: HMSO, 2015).

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

[11] For background to the case see TJ McIntyre, "Data Retention in Ireland: Privacy, Policy and Proportionality," *Computer Law & Security Report* 24, no. 4 (2008): 326–34.

> judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[12]

This need for independence and detachment reflects the conflicting incentives of the police and intelligence/security agencies, who are institutionally unlikely to give adequate weight to privacy concerns. It is particularly important in the context of terrorism, where experience has shown that the executive and legislature can be prone to hasty overreactions. The judiciary, removed from the political cycle and less directly influenced by popular opinion, are best placed to consider whether measures which appear desirable in the short term are in accordance with the law and – in the last resort – whether they are compatible with the longer term interests of a democratic society.[13]

Against this, there are significant limitations to judicial controls, particularly at the stage of the initial authorisation where applications are necessarily based on one-sided information and lack the benefit of an adversarial procedure.[14] This problem is most acute in the area of national security. In criminal matters judges have a special expertise and the use of surveillance evidence in subsequent prosecutions provides an additional opportunity for the trial court to examine whether surveillance should have been authorised. In national security matters, on the other hand, judges are further removed from their training and experience and find it more difficult to look behind intelligence agency claims of threatened harm – especially as security surveillance generally takes place at an earlier stage in an investigation and tends to be more exploratory in its nature.[15] While this can be addressed by having specialist judges or courts – such as the United States Foreign Intelligence Surveillance Court ("FISC") – these in turn present their own risk of regulatory capture as a small pool of judges hearing only from the security agencies may come to lose their objectivity.[16] Also, as surveillance becomes more technically complex judges increasingly lack the specialist knowledge needed to provide adequate oversight.[17]

For these reasons it is important that judicial controls should not exist in isolation but should form part of a wider system of accountability including specialised oversight institutions. In two significant

---

[12] *Klass v. Germany*, application 5029/71, 6 September 1978, para 55.

[13] See e.g. Kent Roach, "Judicial Review of the State's Anti-Terrorism Activities: The Post 9/11 Experience and Normative Justifications for Judicial Review," *Indian Journal of Constitutional Law* 3 (2009): 138.

[14] Iain Cameron, *National Security and the European Convention on Human Rights* (Martinus Nijhoff Publishers, 2000), 157–161.

[15] European Commission for Democracy through Law, "Report on the Democratic Oversight of the Security Services" (Strasbourg, June 11, 2007), 45, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_cdl-ad(2007)016_/3_cdl-ad(2007)016_en.pdf.

[16] *Idem*, 47.

[17] For example, in the US the President's Review Group and the Privacy and Civil Liberties Oversight Board have examined the operation of the FISC and in both cases have concluded that it needs additional technical guidance to carry out its work effectively. See President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Washington, DC, 2013), chapter VI; Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (Washington, DC, January 23, 2014), pt. 8, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

reports both the Venice Commission[18] and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism[19] have recommended that such systems must cover all aspects of the work of intelligence agencies including the interaction between different agencies and the police. Systems which focus on particular instances of surveillance may overlook other threats to privacy such as data mining or the sharing of intercepted communications with other countries.

3. Types of judicial oversight

Where national systems provide for judicial oversight of surveillance this may take place before the surveillance is carried out (*ex ante*) and/or after the fact (*ex post*).[20] Judicial oversight during ongoing surveillance is a feature of some systems (as in the case of investigating magistrates in France) but is less common except in relation to the continuation of existing approvals.[21]

Ex ante control generally takes the form of judicial authorisation – i.e. prior approval of applications for surveillance by police or intelligence services. These authorisation systems vary in their scope, from individualised warrants targeting named suspects to approval of general procedures within which authorities enjoy great discretion as to the individuals and facilities to be targeted.[22] *Ex ante* judicial control will be most effective at safeguarding rights if it involves the application of clear and well-defined rules: where open-ended laws are involved there is a risk – highlighted by the FISC – that a secret body of case law may develop outside the adversarial process and without scrutiny by appellate courts or the wider legal community.[23]

Ex post judicial oversight also varies greatly between national systems. A common form is judicial examination of complaints that an individual has been wrongfully subjected to surveillance, whether through the ordinary courts or a specialist tribunal. While this is an important remedy, it has the disadvantage of being reactive in nature and dependent on the individual being aware of the

[18] European Commission for Democracy through Law, "Report on the Democratic Oversight of the Security Services," 49.

[19] Martin Scheinin, "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism: Compilation of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight" (United Nations General Assembly, May 17, 2010), 8, http://www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/14/46.

[20] See generally European Commission for Democracy through Law, *Report on the Democratic Oversight of the Security Services*, chapter 9.

[21] For an extensive survey of national systems see Cameron, *National Security and the European Convention on Human Rights*, chapter 2.

[22] See in particular the wide discretion permitted by the US FISA Amendments Act of 2008, under which the FISC reviews only the general procedures which the government proposes to use: Glenn Greenwald, "Fisa Court Oversight: A Look inside a Secret and Empty Process," *The Guardian*, June 19, 2013, http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy.

[23] Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *The New York Times*, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

surveillance and being able to access evidence proving abuse.[24] For that reason it will work best in those systems which provide for individuals to be notified after surveillance has ceased.[25]

Another type of *ex post* oversight is the scrutiny of surveillance evidence in criminal prosecutions. Particularly in jurisdictions where there are strict rules of admissibility, the disclosure of surveillance evidence to the defence provides an opportunity to examine the circumstances of the surveillance and to challenge the evidence if it was obtained improperly. In *Uzun v. Germany* the ECtHR identified this as an oversight mechanism in its own right, accepting the state argument that "the possibility to exclude evidence obtained from an illegal GPS surveillance constituted an important safeguard".[26]

This is, however, a relatively weak form of oversight. It is *ad hoc* in that it depends on the accident of whether a prosecution is brought in a particular case and does not necessarily provide any insight into wider practices. It can be avoided by laws which limit surveillance material to intelligence rather than evidential use.[27] It can also be evaded simply by deceiving the court about the origins of evidence, and in 2013 a Reuters report revealed the existence of a practice known as "parallel construction" whereby the US Drug Enforcement Agency (DEA) systematically fabricated the basis on which investigations were carried out in order to conceal from defence lawyers the fact that they had involved warrantless surveillance by the National Security Agency (NSA).[28] Also, it is of less relevance for surveillance carried out by the security services, where it is unlikely that any particular case will end up in court.[29]

---

[24] European Commission for Democracy through Law, "Report on the Democratic Oversight of the Security Services," 55.

[25] As to which see e.g. Paul De Hert and Franziska Boehm, "The Rights of Notification after Surveillance Is over: Ready for Recognition," in *Digital Enlightenment Yearbook 2012*, ed. Jacques Bus et al. (IOS Press, 2012), http://www.vub.ac.be/LSTS/pub/Dehert/408.pdf; Patrick C. Toomey and Brett Max Kaufman, "The Notice Paradox: Secret Surveillance, Criminal Defendants & the Right to Notice," *Santa Clara Law Review* 54 (2014), http://papers.ssrn.com/abstract=2552856.

[26] *Uzun v. Germany*, application 35623/05, 2 September 2010, para. 80.

[27] For example, in the United Kingdom intercept evidence has been made inadmissible by law at least in part to avoid disclosures which might reveal particular surveillance capabilities: Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperPress, 2010), 542–543; Dominic Raab, *Fight Terror, Defend Freedom* (London: Big Brother Watch, 2010), chapter 2, http://www.bigbrotherwatch.org.uk/files/dominicraabbookfinal.pdf; Home Office, *Intercept as Evidence* (London, December 2014), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388111/InterceptAsEvidence.pdf.

[28] John Shiffman and Kristina Cooke, "U.S. Directs Agents to Cover up Program Used to Investigate Americans," *Reuters*, August 5, 2013, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805; Shawn Musgrave, "DEA Teaches Agents to Recreate Evidence Chains to Hide Methods," *MuckRock*, February 3, 2014, https://www.muckrock.com/news/archives/2014/feb/03/dea-parallel-construction-guides/; Brad Heath, "U.S. Secretly Tracked Billions of Calls for Decades," *USA TODAY*, April 7, 2015, http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/.

[29] European Commission for Democracy through Law, "Report on the Democratic Oversight of the Security Services," 46.

Judicial review of surveillance measures can also be regarded as a form of *ex post* oversight. The term judicial review has different meanings in different legal systems but here we focus on what Davis and de Londras term *constitutional* rather than *administrative* judicial review.[30] While administrative judicial review assesses whether particular examples of surveillance are authorised by the relevant law and adopted following appropriate processes, judicial review in the broader constitutional sense asks whether the surveillance law or practice itself is compatible with human rights or fundamental constitutional principles. However, it presents an uphill battle for those who wish to challenge a particular form of surveillance.

The starting point – and indeed the finishing point for many litigants – is the issue of standing. In the United States in particular those challenging mass surveillance have foundered due to an inability to show that they have suffered any injury – leading to the perverse result that secret surveillance laws cannot be challenged precisely because they are secret.[31] In Europe, standing rules vary at the national level but restrictive national rules are mitigated by the possibility of recourse to the ECtHR, where a pragmatic approach to standing ensures that persons "potentially affected by secret surveillance" will be regarded as "victims" for the purpose of the Convention. The alternative, according to the court in *Klass v. Germany*, would be that "the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation".[32]

Judicial review also presents issues of institutional competence and the extent to which the judiciary should defer to the elected branches of government on the necessity of surveillance.[33] However these issues should not be overstated. Roach points out that the claims of the executive and legislature are often exaggerated and the executive in particular has an incentive to use secrecy as a tool to avoid accountability for failure and abuses.[34] Secret surveillance can also involve an aggressive interpretation of laws to achieve results which were not contemplated by the legislature. For example, in June 2013 the primary author of the Patriot Act (then chairman of the House Judiciary Committee, Jim Sensenbrenner) wrote that the bulk collection of telephone records revealed by Edward Snowden was "an abuse of that law" which relied "on an unbounded interpretation of the act that Congress never intended".[35] In these circumstances judicial review serves an important democratic purpose by publicising the manner in which the law is actually being applied and ensuring that any expansion of surveillance is explicitly authorised by lawmakers. Finally, judicial review of surveillance is particularly well suited to Roach's model of a dialogue between courts and the legislature.[36] In most cases where laws are struck down the finding is not that the

[30] Fergal Davis and Fiona de Londras, "Counter-Terrorist Judicial Review: Beyond Dichotomies," in *Critical Debates on Counter-Terrorist Judicial Review)*, ed. Fergal Davis and Fiona de Londras (Cambridge: Cambridge University Press, 2014).

[31] See e.g. *Clapper v. Amnesty International USA* 133 S. Ct. 1138 (2013).

[32] *Klass v. Germany*, application 5029/71, 6 September 1978, para. 36.

[33] As to which see e.g. Roach, "Judicial Review of the State's Anti-Terrorism Activities"; Davis and de Londras, "Counter-Terrorist Judicial Review."

[34] Roach, "Judicial Review of the State's Anti-Terrorism Activities."

[35] Jim Sensenbrenner, "This Abuse of the Patriot Act Must End," *The Guardian*, June 9, 2013, http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end.

[36] Roach, "Judicial Review of the State's Anti-Terrorism Activities."

surveillance technique itself is illegitimate but rather that the law is insufficiently precise or the procedural safeguards inadequate. In these cases the legislature may respond with a better tailored law if it still considers the particular form of surveillance necessary.

There is also the possibility of *ad hoc* judicial oversight – for example where a sitting or retired judge is appointed to chair an investigation into a particular scandal. This has been common in Ireland where allegations of wrongful police surveillance have featured in a number of judge-led inquiries.[37] While this type of oversight may be the best available in a particular context, the need to resort to it is itself a sign that there are failings in the existing oversight mechanisms.

4. Judicial oversight as a requirement in Irish law

The Irish courts have not directly[38] considered whether judicial oversight of surveillance is constitutionally required, but there is some precedent from the analogous area of search warrants. The early cases used a formalistic analysis, holding that the decision to issue a search warrant was "part of the investigative process" so that it was "executive rather than judicial in nature" and did not require prior judicial approval notwithstanding that it authorised an invasion of the constitutional right to privacy.[39] Following this reasoning, a number of laws gave the power to issue search warrants to non-judicial officials and even to the police themselves.[40]

Recently, however, the Supreme Court has taken a different approach which focuses on the role of independent control in protecting fundamental rights. In *Damache v. DPP*[41] the applicant challenged the constitutionality of what were in effect "self-service search warrants", whereby a senior police officer could issue a search warrant provided that they had a "reasonable ground for believing that evidence [relating to a terrorist offence] is to be found" in any location.[42] At first instance Kearns P. upheld such warrants on the basis that:

[37] Frederick Morris, "Fifth Report of the Tribunal of Inquiry Set Up Pursuant to the Tribunal of Inquiry (Evidence) Acts 1921-2002 into Certain Gardaí in the Donegal Division" (Dublin, 2006), http://www.justice.ie/en/JELR/Morris5thRpt.pdf/Files/Morris5thRpt.pdf; John D Cooke, "Inquiry into Reports of Unlawful Surveillance of Garda Síochána Ombudsman Commission" (Dublin, 2014), http://www.merrionstreet.ie/en/wp-content/uploads/2014/06/GSOC-Report-Final-REDACTED.pdf; Nial Fennelly, "Interim Report of the Commission of Investigation into Certain Matters Relative to An Garda Síochána and Other Persons" (Dublin, November 2014), http://www.taoiseach.gov.ie/eng/Publications/Publications_2015/Fennelly_Commission_Interim_Report.pdf.

[38] In *DPP v. Murphy* [2005] IECCA 1 the Court of Criminal Appeal assumes without discussion that prior judicial authorisation is not required in the case of police access to telephone records. Compare *Schrems v Data Protection Commissioner* [2014] IEHC 310 in which Hogan J. states that "appropriate and verifiable safeguards" would be required – but does not specify prior judicial authorisation or indeed judicial oversight.

[39] *Ryan v. O'Callaghan*, unreported, High Court, Barr J., 22 July 1987.

[40] Law Reform Commission, *Consultation Paper: Search Warrants and Bench Warrants* (Dublin, 2009), chapter 4, http://www.lawreform.ie/_fileupload/consultation%20papers/cpsearchwarrantsandbenchwarrants.pdf.

[41] [2011] IEHC 197 (High Court); [2012] IESC 11 (Supreme Court).

[42] See generally Paul MacMahon, "Self-Service Search Warrants and International Terrorism: Lessons from *Damache v. DPP*," *Irish Law Journal* 1 (2012): 2.

> "the security demands of countering international terrorism are of a quite different order to those which apply in what might be described as routine criminal offences... The international terrorism of the modern age is a sophisticated, computerised and fast moving process where crucial evidence may be lost in minutes or seconds in the absence of speedy and effective action by police authorities."

On appeal, the Supreme Court did not adopt this uncritical view of terrorism exceptionalism. Instead the court identified a general constitutional principle that search warrants should only be issued by an independent person, holding that:

> "For the process in obtaining a search warrant to be meaningful, it is necessary for the person authorising the search to be able to assess the conflicting interests of the State and the individual in an impartial manner. Thus, the person should be independent of the issue and act judicially."[43]

Applying this principle, the power was found invalid insofar as it allowed for a member of the police investigating team to grant a search warrant for the home (which has special protection under the Irish constitution[44]) without there being any urgency or other exceptional circumstances. Significantly, the decision went further than merely requiring that warrants are issued by police who are not personally involved in an investigation. In addition to the requirement that the person issuing the warrant should "act judicially" the court also held that "in the circumstances of this case a person issuing the search warrant should be independent of the Garda Síochána [the police force], to provide effective independence".[45] This is a requirement of *institutional*, not merely *personal*, independence and requires that a power to issue search warrants – at least in respect of the home – should only be exercised by an outside authority except in cases of urgency.

The later judgment of the Court of Criminal Appeal in *DPP v. Cunningham*[46] has elaborated on this requirement. In *Cunningham* Hardiman J. (a member of the panel who decided *Damache*) described the self-issued warrant procedure as being:

> "little more than a convenient and decorous formality which, absent the fundamental safeguards we have described of third party supervision and documentation, was in truth often little better than a warrantless search of a private dwelling."

Hardiman J. went on to explain *Damache* as reflecting the reasoning in the German Constitutional Court decision of 20th February 2001[47] (finding a warrantless search of a home unconstitutional) which he summarised as holding that:

> "any derogations from the fundamental constitutional protection must be interpreted restrictively, pointing out that an independent (judicial) examination of the necessity for a search was likely to limit the interference with this fundamental right by ensuring it was confined to that which was demonstrably necessary in any given case. Such a requirement promoted transparency, since the objective necessity for the search has to be explained to an independent third party and appropriately documented so that it can be reviewed later."

[43] *Damache v. DPP* [2012] IESC 11, para. 51.

[44] Article 40.5 refers to the "inviolability of the dwelling".

[45] *Damache v. DPP* [2012] IESC 11, para. 54.

[46] [2012] IECCA 64.

[47] BVerfG, 2 BvR 1444/00.

While *Damache* and *Cunningham* did not apply directly to surveillance, the case they make for prior judicial authorisation is stronger again in that context. Ongoing surveillance is often much more invasive and revealing than a once-off search of premises and, because the individual is not aware of the surveillance, it is also more likely to escape subsequent review. In addition, the High Court, relying on German authority, has recently recognised that the interception of communications generated within the home "directly engages the inviolability of the dwelling" which suggests that the *Damache* principle of prior independent authorisation should apply to such surveillance also.[48] These cases may eventually lead to a ruling that the Irish constitution requires *ex ante* judicial control of communications surveillance – for the time being, however, the issue remains open.

5. Judicial oversight as a requirement under the ECHR

The ECtHR has an extensive body of case law establishing that both the interception of communications and the retention of communications data constitute an interference with the right to privacy.[49] For communications surveillance to be permissible under Article 8(2) it must therefore be "in accordance with the law" and "necessary in a democratic society" to pursue one or more of the legitimate aims referred to in that paragraph. While Article 8 does not itself specify procedural safeguards, the Court has interpreted the principle of legality in a way which builds in such requirements.[50] The cases are not always internally consistent, making it difficult to extract general rules, but for the most part they have insisted on two closely related principles.

The first 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

[48] *Schrems v Data Protection Commissioner* [2014] IEHC 310, para. 48 *per* Hogan J.: "One might add that the accessing by State authorities of private communications generated within the home – whether this involves the accessing of telephone calls, internet use or private mail – also directly engages the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution. As it happens, by one of those accidents of legal history, these very same words are also contained in Article 13(1) of the German Basic Law ("inviolability of the dwelling") ("unverletzlichkeit der Wohnung"). It is, accordingly, of interest that the German Constitutional Court has held that the accessing by state authorities of otherwise private communications within the home also engages that more or less identically worded guarantee of inviolability of the dwelling which is contained in Article 13(1) of the Basic Law. Indeed that Court went further and found that legislation providing for the interception and surveillance of communications partly unconstitutional because it provided for a disproportionate interference without adequate safeguards with that very guarantee of inviolability of the dwelling in Article 13(1) of the Basic Law: see Anti-Terrorism Database Law decision (1 B v R 1215/07) (April 24, 2013) at paras. 93 et seq."

[49] See e.g. Ian Brown and Douwe Korff, "Terrorism and the Proportionality of Internet Surveillance," *European Journal of Criminology* 6, no. 2 (March 1, 2009): 119–34; Toon Moonen, "Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights," *Pace International Law Review Online Companion* 1, no. 9 (2010): 97; Nora Ni Loideain, "Surveillance of Communications Data and Article 8 of the European Convention on Human Rights," in *Reloading Data Protection*, ed. Serge Gutwirth, Ronald Leenes, and Paul De Hert (Dordrecht: Springer Netherlands, 2014).

[50] See in particular *Klass v. Germany*, application 5029/71, 6 September 1978; *Malone v. United Kingdom*, application 8691/79, 2 August 1984; *Weber and Saravia v. Germany*, application 54934/00, 29 June 2006; and *Kennedy v. United Kingdom*, application 26839/05, 18 May 2010.

interference".[51] A series of cases have developed this to identify an extensive set of issues which must be addressed in legislation. *Weber and Saravia v. Germany* summarises these 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."[52]

The second principle 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. As explained in *Uzun v. Germany*:

> "This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law."[53]

Although these principles have the same origin and are sometimes treated interchangeably by the ECtHR they nevertheless operate in very different ways. The requirement of foreseeability sets a prescriptive checklist: legislation which permits surveillance must, at a minimum, address a series of specified points to comply with Article 8. Whether there are adequate guarantees against abuse, however, is a more open-ended question which looks at the totality of the regulatory system. Once there is some form of independent supervision, the precise control mechanisms used – such as *ex ante* or *ex post* judicial controls, parliamentary oversight or notification of those affected – are factors to be taken into account but generally not individually decisive.[54]

There is also a significant overlap between the guarantees against abuse required by Article 8 and the right to an effective remedy required by Article 13, and the cases have not always differentiated between the two concepts. As Cameron puts it:

> "The Convention organs draw no hard and fast line between 'control' mechanisms, in the sense of prior, or ongoing, authorising, or vetoing, of a surveillance measure, and 'review'/'accountability' mechanisms, in the sense of *post hoc* supervision which can alter or cancel the measure, provide monetary compensation for it, or simply criticize arrangements in general or the measure in particular… The approach of the Convention organs instead is usually global: all the safeguards and remedies are added up and a conclusion pops out."[55]

To what extent, then, do Articles 8 and 13 mandate judicial oversight of surveillance?

---

[51] *Weber and Saravia v. Germany*, application 54934/00, 29 June 2006, para. 94.

[52] Idem, para. 95.

[53] *Uzun v. Germany*, application 25623/05, 2 September 2010, para 63.

[54] See e.g. *Klass v. Germany*, application 5029/71, 6 September 1978, para. 56.

[55] Cameron, *National Security and the European Convention on Human Rights*, 126–127.

As regards *ex ante* and ongoing oversight, we have already seen that *Klass v. Germany*[56] expressed a strong preference, but not a requirement, for judicial control of surveillance of communications. This remains the general approach which later cases have taken across both criminal and national security surveillance. Although there are some suggestions in the cases that criminal surveillance should be subject to more stringent requirements (*Huvig v. France*[57] and *Kruslin v. France*[58] in particular state that national law should define "the categories of people liable to have their telephones tapped *by judicial order*"[59]) this has not yet been generalised to a wider requirement for *ex ante* judicial approval.[60] Indeed, the case law has not always insisted that *ex ante* authorisation should be independent. While *Iordachi v. Moldova*[61] stated that "the body issuing authorisations for interception should be independent" the Court has also upheld the system in *Kennedy v. United Kingdom*[62] in which interception warrants are issued by the Home Secretary – a member of the executive – on the basis that extensive *ex post* oversight is available through the Investigatory Powers Tribunal and the Interception of Communications Commissioner.[63]

That said, there is an important recent ruling of the ECtHR in *Telegraaf Media v. the Netherlands*[64] which has the effect of requiring *ex ante* (quasi-) judicial authorisation in relation to the media. That case involved targeted surveillance of journalists, including telephone tapping, in order to identify the sources behind documents leaked from the Netherlands secret service (AIVD). It therefore implicated both the right to privacy and the right to freedom of expression, presenting a clash between the general rule under Article 8 (*ex ante* judicial/independent approval not required) and the specific jurisprudence in relation to protection of journalistic sources under Article 10 (that there must be a prior independent review assessing the public interest before the identity of sources is revealed[65]). Because the surveillance was authorised by the Minister of the Interior[66] it did not meet the Article 10 requirement of "prior review by an independent body with the power to prevent or terminate it"[67] and in the circumstances the *ex post* review mechanisms were inadequate as they

[56] *Klass v. Germany*, application 5029/71, 6 September 1978.

[57] *Huvig v. France*, application 11105/84, 24 April 1990.

[58] *Kruslin v. France*, application 11801/85, 24 April 1990

[59] *Huvig v. France*, application 11105/84, 24 April 1990, para. 34; *Kruslin v. France*, application 11801/85, 24 April 1990, para. 35. Emphasis added.

[60] Stefan Sottiaux, *Terrorism and the Limitation of Rights: The ECHR and the US Constitution*, Human Rights Law in Perspective, v. 12 (Oxford ; Portland, OR: Hart, 2008), 294–295.

[61] *Iordachi v. Moldova,* application 25198/02, 10 February 2009, para. 40 citing *Dumitru Popescu v. Romania (No. 2)*, application 71525/01, 26 April 2007.

[62] *Kennedy v. United Kingdom*, application 26839/05, 18 May 2010.

[63] *Idem*, para. 167.

[64] *Telegraaf Media v. The Netherlands*, application 39315/06, 22 November 2012.

[65] *Sanoma Uitgevers BV v. the Netherlands*, application 38224/03, 14 September 2010.

[66] Or perhaps an official of the AVID – see *Telegraaf Media v. The Netherlands*, application 39315/06, 22 November 2012, para. 100.

[67] *Telegraaf Media v. The Netherlands*, application 39315/06, 22 November 2012, para. 100.

could not "restore the confidentiality of journalistic sources once it is destroyed".[68] Accordingly the Court found that the surveillance violated both Articles 8 and 10.

The ruling in *Telegraaf Media* will require significant changes to the legal framework around police and national security surveillance in many European countries and, more generally, suggests that the Court is willing to require *ex ante* judicial or quasi-judicial review of surveillance practices where the category of information targeted enjoys special protection under the ECHR. In this it echoes *Kopp v. Switzerland*[69] where telephone tapping of calls to and from a lawyer was found to violate Article 8, in part because the process for screening out legally privileged recordings was left to the discretion of a post office official without judicial control. According to the Court:

> *"Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence."*[70]

Turning to *ex post* oversight, we have already seen that *Klass v. Germany* accepted that non-judicial supervisory bodies could provide adequate guarantees against abuse for the purposes of Article 8 where they were "independent of the authorities carrying out the surveillance", "vested with sufficient powers and competence to exercise an effective and continuous control" and had a "democratic character" which provided representation for opposition parties.[71] Similarly, the Court has held that in principle an adequate remedy for the purposes of Article 13 is possible through non-judicial mechanisms.[72] However the Grand Chamber in *Klass v. Germany* also stated that, given the special dangers of secret surveillance, "effective control… should normally be assured by the judiciary, at least in the last resort"[73] indicating that the individual should ultimately have the ability to bring an action before the courts. This was, according to the Grand Chamber, "inextricably linked" to the question of subsequent notification as "there is in principle little scope for recourse to the courts" unless the individual "is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality".[74]

Klass v. Germany and subsequent cases have therefore developed a principle of notification after surveillance as a means of ensuring a residual form of *ex post* judicial oversight. This has recently been considered in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*[75] which summarised it as requiring that "as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to

---

[68] *Idem*, para. 101.

[69] *Kopp v. Switzerland*, application 23224/94, judgment of 25 March 1998.

[70] *Idem*, para. 74.

[71] *Klass v. Germany*, application 5029/71, 6 September 1978, para. 56.

[72] *Leander v. Sweden*, application 9248/81, 26 March 1987; *Silver and others v. United Kingdom*, applications 5947/72 et al., 25 March 1983.

[73] *Klass v. Germany*, application 5029/71, 6 September 1978, para. 55.

[74] *Idem*, para. 57.

[75] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, application 62540/00, 28 June 2007.

the persons concerned". [76] In that case the Court found that Bulgaria was in breach of both Article 8 and Article 13 where national laws on special means of surveillance failed to provide for any notification and expressly prohibited disclosure of information as to whether a person had been subjected to surveillance. Significantly, the decision appears to treat subsequent notification as a mandatory requirement in its own right, not merely a factor to be taken into account in determining if the overall system of safeguards against abuse is adequate. If this interpretation is confirmed by later cases it will require significant reform in those jurisdictions – such as the United Kingdom and Ireland – where notification has hitherto not been required.[77]

6. Judicial oversight as a requirement under the EU Charter of Fundamental Rights

To what extent does the EU Charter of Fundamental Rights require greater judicial oversight of surveillance, going beyond merely paralleling the ECHR? To answer we must first consider how the Charter and ECHR interact. Article 52(3) of the Charter provides that:

> "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

There is a continuing debate as to the precise legal relationship this creates between the two regimes, but the net effect is that EU law now takes the ECHR as a floor rather than a ceiling.[78] This is particularly important in the area of surveillance which implicates the right to data protection under Article 8 of the Charter. That right overlaps with the Article 7 right to privacy but is nevertheless a distinct right which has no direct counterpart under the ECHR – making it inevitable that there will be some divergence between ECHR and Charter standards.[79]

This point has now been highlighted by the decision of the CJEU in *Digital Rights Ireland* finding that the Data Retention Directive was disproportionate under Articles 7 and 8 of the Charter.[80] While the CJEU found fault with many aspects of the Directive, one of the most significant was the lack of *ex*

[76] *Idem*, para. 90.

[77] On notification generally see Cameron, *National Security and the European Convention on Human Rights*, 161–162; De Hert and Boehm, "The Rights of Notification after Surveillance Is over: Ready for Recognition"; 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.

[78] See e.g. Tobias Lock, "The ECJ and the ECtHR: The Future Relationship between the Two European Courts," *The Law & Practice of International Courts and Tribunals* 8, no. 3 (2009): 375.

[79] For analysis of the ways in which the data protection right differs from the privacy right see 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.

[80] As to which see e.g. Judith Rauhofer and Daithí Mac Síthigh, "The Data Retention Directive Never Existed," *SCRIPTed* 11, no. 1 (April 2014), http://script-ed.org/?p=1480; Marie-Pierre Granger and Kristina Irion, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland-Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection," *European Law Review* 39, no. 4 (2014): 835.

ante judicial (or quasi-judicial) approval before retained data could be accessed. In a passage going significantly further than the Article 8 ECHR jurisprudence, the Court stressed that:

> "*Above all*, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."[81]

This is significant in several regards. First, it puts controls for access to communications data largely on a par with those for the interception of the content of communications. This departs from ECtHR decisions such as *PG and JH v. United Kingdom*[82] which saw communications data as significantly less sensitive and therefore upheld systems in which "metering" information could be disclosed to police by phone companies without any prior independent approval. To the contrary, the CJEU treats communications data as itself particularly revealing and therefore deserving of the highest level of protection.

Second, by insisting on prior review by a court or independent body it rejects the approach in *Kennedy v. United Kingdom* which, as we have seen, accepted that *ex ante* authorisation to intercept communications could be given by a politician provided that *ex post* controls were sufficiently rigorous. The requirement for prior independent review is itself a mandatory requirement under the Charter, independent of whatever other safeguards might be in place.[83]

Third, and perhaps most importantly, the principles elaborated by the CJEU are not confined to EU legislation and will demand higher standards from national surveillance laws also. While the Charter does not generally apply to member state actions, it will do so when member states are "implementing" EU law.[84] As interpreted by the CJEU in *Fransson*[85] and *Pfleger*,[86] this will include "all situations governed by" or "within the scope of" EU law, including derogations from EU law.[87] In practice, this extends the Charter to cover most national surveillance laws, as these will generally involve member states relying on either the derogations in Article 15 of the e-Privacy Directive[88] (to intercept communications or capture communications data) or else the derogations in Article 13 of

[81] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, para. 62, emphasis added.

[82] *PG and JH v. United Kingdom*, application 44787/98, 25 September 2001.

[83] In *Davis v. Home Secretary* [2015] EWHC 2092 (Admin) the English High Court accepted this interpretation in finding that the Data Retention and Investigatory Powers Act 2014 was inconsistent with EU law.

[84] 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.

[85] Case C-617/10, *Åklagaren v. Hans Åkerberg Fransson.*

[86] Case C-390/12, *Pfleger and others*.

[87] *Idem,* paras. 30-37.

[88] Directive 2002/58/EC.

the Data Protection Directive[89] (to collect and process personal data).[90] This was confirmed by the *Privacy First*[91] case in the Netherlands where the Hague District Court found the Dutch Telecommunications Data Retention Law to be within the scope of the Charter and therefore, applying *Digital Rights Ireland*, in violation of Articles 7 and 8 of the Charter. In the same way, the English High Court in *Davis v. Home Secretary*[92] held that the Data Retention and Investigatory Powers Act 2014, although a domestic measure adopted in response to *Digital Rights Ireland*, was within the scope of EU law and similarly inconsistent with the Charter.

It is clear, therefore, that the CJEU has gone significantly further than the ECtHR as regards the requirement for *ex ante* judicial controls. While the full implications of the *Digital Rights Ireland* decision have yet to be teased out, it certainly marks a significantly greater role for EU law in assessing the fundamental rights compatibility of surveillance. It will be particularly important in jurisdictions such as Ireland and the United Kingdom where interception of communications is carried out on the basis of a ministerial warrant with no prior judicial authorisation: it is unsustainable that there should be a lower standard for access to the content of communications than for access to communications data. At a practical level we can expect that challenges to surveillance laws in the EU will increasingly be framed in terms of Charter as well as ECHR norms. In addition to (possibly) more expansive rights under the Charter, this will also 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, disapplying national procedural rules if necessary.[93]

7. Case study: judicial oversight of data retention in Ireland

So far we have looked at judicial oversight in the abstract. But what might we learn from examining a particular system in detail? In this section we consider the practical operation of data retention in Ireland – ultimately reaching the conclusion that the combined effect of open-ended legislation and inconsistent implementation has provided the appearance, but not the reality, of effective safeguards.

---

[89] Directive 95/46/EC.

[90] See in particular Steve Peers, "Are National Data Retention Laws within the Scope of the Charter?," *EU Law Analysis*, July 10, 2014, http://eulawanalysis.blogspot.co.uk/2014/04/are-national-data-retention-laws-within.html; Steve Peers, "Does the UK's New Data Retention Bill Violate the EU Charter of Fundamental Rights?," *EU Law Analysis*, July 10, 2014, http://eulawanalysis.blogspot.ie/2014/07/does-uks-new-data-retention-bill.html. Though note that surveillance measures which are *solely* for national security purposes may not be within the scope of the Charter as they may fall entirely outside EU competence.

[91] Case number C/09/480009 / KG ZA 14/1575, 11 March 2015. See 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. The court also held that the national law was within the scope of the Charter insofar as it imposed a restriction on the freedom to provide services.

[92] [2015] EWHC 2092 (Admin).

[93] For example, in the domestic proceedings in the *Digital Rights Ireland* case the High Court accepted that national rules on standing and security for costs had to be relaxed where their enforcement would frustrate the enforcement of Charter rights. See *Digital Rights Ireland Ltd v Minister for Communication* [2010] IEHC 221.

Judicial involvement in the data retention system was first introduced in the Criminal Justice (Terrorist Offences) Act 2005 and was renewed in the Communications (Retention of Data) Act 2011. These provide for *ex post* judicial oversight only.[94] The initial request to disclose retained data does not involve any outside approval, so that the Garda Síochána (police force), the Permanent Defence Force (army), the Revenue Commissioners and the Competition and Consumer Authority can obtain retained telephone and internet data based solely on an internal authorisation procedure.[95]

Judicial involvement is provided by an extension of the system previously created to oversee interception of communications.[96] There are two distinct judicial roles. For general oversight a "designated judge" – a judge of the High Court, nominated by the President of the High Court – is given the functions of keeping the operation of the Act under review, ascertaining whether the authorities are complying with its provisions and providing an annual report to the Taoiseach (Prime Minister) including such matters as they think appropriate. The designated judge is given the power to investigate any case in which a request for data has been made, to access and inspect any official document relating to the request, and to communicate with the Taoiseach, Minister for Justice Equality or Data Protection Commissioner if they consider it desirable to do so.[97]

A redress mechanism involves a "Complaints Referee" who is appointed by the Taoiseach for a five year term and during that time enjoys the same tenure as a High Court judge. The qualification for appointment is the same as that for appointment as a judge, but in practice all holders of the office to date have been sitting judges of the Circuit Court.[98] The Complaints Referee is empowered to investigate complaints that data relating to a person has been accessed following a disclosure request, and if they find that a disclosure request was wrongfully made they must notify the complainant of their finding and make a report to the Taoiseach. They may also order that the data be destroyed and that compensation be paid. The Complaints Referee has powers to access and inspect any official records and to request any information relating to a disclosure request. Significantly, the mechanism is not exclusive – it remains open to individuals to bring an action for wrongful access to data before the ordinary courts or to complain to the Data Protection Commissioner.[99]

When introduced, these provisions were described by the Minister for Justice as "strict new safeguards" which were intended to address the possibility that the ECtHR "might well require us to extend that kind of independent supervisory mechanism from phone tapping to data communication-type circumstances".[100] On paper they might well appear adequate. In practice, however, they have been less satisfactory.

---

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

[95] Section 6, Communications (Retention of Data) Act 2011; section 89, Competition and Consumer Protection Act 2014.

[96] Under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

[97] Section 12, Communications (Retention of Data) Act 2011; section 8, Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

[98] Section 9, Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

[99] Section 10, Communications (Retention of Data) Act 2011.

[100] *Dáil Debates*, 23 February 2005, http://debates.oireachtas.ie/dail/2005/02/23/00010.asp.

Starting with the Complaints Referee mechanism, it seems that there has never been a successful complaint of wrongful access to data[101] but beyond that almost nothing is known about its operation. Complaints and decisions are private and there is no publicly available information as to the number of complaints which have been made nor the way in which the Complaints Referee carries out his function. The fact that there has never been a finding in favour of a complainant may reflect scrupulous operation of the system, or it may reflect the fact that under Irish law there is no requirement for notification after the fact, leaving individuals unaware that their communications have been monitored and unable to bring a complaint.

There is little more transparency in the case of the designated judge. Since the creation of the role, the annual reports have consisted almost exclusively of bland reassurances – a few paragraphs which recite that on a particular day certain (unspecified) documents were inspected, certain (unspecified) queries answered and as a result the judge is satisfied that the relevant authorities are in compliance with the law.[102] The reports have provided no indication as to the methodology used (are random disclosure requests chosen and audited; are internal systems reviewed?), no statistics[103] as the use of data retention, no indication of the circumstances in which it is being used, and no indication of the internal safeguards in place to prevent abuse or address errors. Particularly when the oversight role is a part-time function of a busy judge with no staff, specialist training or technical advisors, this lack of detail does not instil confidence and suggests an over-reliance on the entities supposedly being monitored.

Until recently the formulaic nature of these reports made it difficult to assess the effectiveness of the designated judge. Recently, however, two developments have exposed significant failings. In 2010 newspaper reports revealed that a detective sergeant in the Crime and Security Division abused the data retention system to spy on her ex-boyfriend.[104] This came to light due to his becoming suspicious – not due to any internal safeguards – and indicated a very serious flaw in the system, given that she was not authorised to make such requests. Remarkably, the only response of the designated judge in the next annual report was to say that "I am satisfied that the full extent of the alleged non-compliance with the Act has been rigorously investigated and fully understood and all appropriate steps taken to ensure future compliance". No account was given as to how the sergeant was able to circumvent the requirement of authorisation by a Chief Superintendent, or whether a Chief Superintendent might have been at fault in approving a request from her without due diligence. It should be noted that the incident also highlights failings in Garda discipline: the

[101] *Dáil Debates,* Written Answers, 4 March 2008, 122-123, http://debates.oireachtas.ie/dail/2008/03/04/unrevised2.pdf

[102] The annual reports of the designated judge and other official materials cited in this case study are available at Digital Rights Ireland, "Surveillance Library," accessed March 25, 2015, https://www.digitalrights.ie/irish-surveillance-documents/.

[103] Section 9 of the Communications (Retention of Data) Act 2011 provides for statistics to be provided to the European Commission by the Minister for Justice, but only to the extent required by the Data Retention Directive.

[104] Larissa Nolan, "Garda Detective Quizzed for 'Spying on Her Ex,'" *The Mail on Sunday*, June 27, 2010; Mark Tighe, "Garda Accused of Bugging Her Ex-Boyfriend," *The Sunday Times*, February 20, 2011.

sergeant was not prosecuted for this offence, and instead was transferred to another sensitive role in the Special Branch (national security unit).[105]

Further concerns were raised in 2014 when the Data Protection Commissioner (DPC) published an audit into the handling of information in the Garda.[106] That audit identified a number of problems in relation to data retention, all of which the Designated Judge had failed to identify. Most fundamentally, the DPC found that there was a systematic practice of retrospectively rubberstamping requests whereby a "request is made without the Chief Superintendent's knowledge and signed/authorised retrospectively by the Chief Superintendent".[107] This practice essentially negated the statutory requirement that a request should only be made following consideration by a senior garda. The failure of the designated judge to identify such a deliberate and well established breach of the legislation – particularly after the 2010 incident – undermines any confidence in the oversight system.[108]

It should be said, however, that these failings are only partly the result of the legislation itself – the statutory powers are wide enough that many of these points could be addressed if the designated judge and Complaints Referee took a more expansive approach. There is a very similar designated judge provision under the Criminal Justice (Surveillance) Act 2009, which regulates the use of surveillance devices such as covert video cameras and GPS. The statutory language is almost identical in setting out the oversight functions.[109] Despite this, the designated judges under the 2009 Act have made significantly greater use of their powers. Their annual reports are considerably more detailed, generally running to 17 to 30 pages, including statistics as to the number of cases where surveillance has been used and a general assessment of its use.[110] They have also taken an active role in carrying out reviews – choosing a random selection of files, assessing the merits of the decision to use surveillance in each case and in some cases reviewing the surveillance evidence itself.

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

8. Conclusion

[105] John Mooney, "Garda Who Spied on Her Boyfriend Will Keep Job," *The Sunday Times*, August 14, 2011, http://www.thesundaytimes.co.uk/sto/news/ireland/News/Irish_News/article701376.ece.

[106] Data Protection Commissioner, "An Garda Síochána: Final Report of Audit," March 2014, http://www.garda.ie/Documents/User/An%20Garda%20S%C3%ADoch%C3%A1na%20ODPC%20Report%20Final.pdf.

[107] *Idem*, 64.

[108] The designated judge also failed to identify that requests were being made to companies who were not within the scope of the legislation: *Idem*, 63.

[109] Section 12, Criminal Justice (Surveillance) Act 2009.

[110] These annual reports are available at Digital Rights Ireland, "Surveillance Library."

Arguments for increased safeguards have become more important as technological advances reduce the cost and increase the impact of surveillance. As Alito J. noted in *United States v. Jones*[111] these developments have the effect of removing what was previously a self-enforcing guarantee of proportionality:

> "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely under-taken… Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources."[112]

Increased judicial oversight – particularly *ex ante* authorisation – offers the prospect of compensating, at least in part, for the reduced cost and greater technical ease of surveillance. We have seen that the European legal systems discussed in this chapter are moving towards requirements of greater judicial controls and we can see similar developments on the other side of the Atlantic in cases such as *United States v. Jones*[113] (GPS tracking), *Riley v. California*[114] (warrantless searches of mobile phones) and *R v. Spencer*[115] (access to ISP held user data) where the United States and Canadian Supreme Courts have significantly extended the circumstances in which judicial permission is required before surveillance can be deployed or information accessed.[116] At the time of writing there are also two important cases pending before the ECtHR in which civil society coalitions hope to persuade the Court to expand judicial oversight throughout the surveillance process – by arguing that the initial authorisation and overall supervision of secret surveillance measures must be by a judge (*Szabó and Vissy v. Hungary*[117]) and by seeking the recognition of notification after surveillance as an essential safeguard and remedy in all systems (*Lüütsepp v Estonia*[118]).

At the same time, we have also seen from the Irish experience that effective judicial oversight requires more than just judicial involvement – it requires thought as to what that involvement seeks to achieve, what resources are available and whether a particular function is best assigned to a judge. It is significant but not surprising that the audit by the Data Protection Commissioner identified issues which the designated judge did not. A generalist judge cannot be expected to have the specialist knowledge necessary to assess surveillance systems without either training or technical advisors. Larger jurisdictions may have better provisioned supervisory entities with in house expertise – such as the UK Interception of Communications Commissioner's Office – but in a small jurisdiction like Ireland it would be desirable for the designated judge to liaise with the data

[111] 132 S. Ct. 945 (2012).

[112] *Idem,* 963-964.

[113] 132 S. Ct. 945 (2012).

[114] 134 S. Ct. 2473 (2014).

[115] 2014 SCC 43, [2014] 2 S.C.R. 212.

[116] Though compare *R v. Fearon* 2014 SCC 77, [2014] S.C.R. 621, permitting a warrantless search of a mobile phone incident to arrest.

[117] Application 37138/14.

[118] Application 46069/13.

protection authority while carrying out this function.[119] Another aspect highlighted by the Irish experience is the way in which different judges can have very different conceptions of their oversight roles. One concern is that a judge may see the oversight role as limited to narrow questions of legality, to the detriment of broader issues of policy, proportionality and effectiveness. In this context it will be helpful to specify the judicial role in some detail in legislation – and again it will be useful to involve data protection authorities who can be expected to have a broader perspective and who will be better equipped to look at wider issues such as subsequent use of acquired data.[120]

[119] Particularly when Irish law explicitly envisages this: section 12(4), Communications (Retention of Data) Act 2011.

[120] As to the limits of data protection in relation to national security surveillance see Article 29 Data Protection Working Party, "Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes," December 5, 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.