Submission

on the

Communications (Retention of Data) Bill 2009, as initiated

November 2009

Contents

The ICCL wishes to acknowledge the assistance of Colette Bennett, Solicitor, in the preparation of this submission.

About the Irish Council for Civil Liberties (ICCL)

The Irish Council for Civil Liberties (ICCL) is Ireland's leading independent human rights watchdog, which monitors, educates and campaigns in order to secure full enjoyment of human rights for everyone.

Founded in 1976 by Mary Robinson and others, the ICCL has played a leading role in some of the most successful human rights campaigns in Ireland. These have included campaigns resulting in the establishment of an independent Garda Síochána Ombudsman Commission, the legalisation of the right to divorce, more effective protection of children's rights, the decriminalisation of homosexuality and introduction of enhanced equality legislation.

We believe in a society which protects and promotes human rights, justice and equality.

What we do

- Advocate for positive changes in the area of human rights;
- Monitor Government policy and legislation to make sure that it complies with international standards;
- Conduct original research and publish reports on issues as diverse as equal rights for all families, the right to privacy, police reform and judicial accountability;
- Run campaigns to raise public and political awareness of human rights, justice and equality issues;
- Work closely with other key stakeholders in the human rights, justice and equality sectors.

For further information contact:

Irish Council for Civil Liberties (ICCL)
9-13 Blackhall Place
Dublin 7
Tel: +353 1 799 4504
Email: info@iccl.ie
Website: www.iccl.ie

1. Introduction

The Irish Council for Civil Liberties (ICCL) notes with interest the publication of the Communications (Data Retention) Bill 2009[1] as a proposed mechanism to transpose Directive 2006/24/EC (Data Retention).[2] The Data Retention Directive requires EU governments to retain data for assistance in the investigation, detection and prosecution of serious crime[3] and covers both telephones and the internet.

Although aware of the benefits accruing for law enforcement agents when particular data is retained, the ICCL is concerned that the proposals in the Bill do not give appropriate weight to privacy considerations. Communications data may constitute personal data under the Data Protection Acts 1988 – 2003 and falls within the ambit of "private life" under Article 8 of the European Convention on Human Rights (ECHR).[4] Such private communications also attract protection under the Constitution.[5]

The retention of numbers dialled, length of calls, the location of the transmission, as well as email and internet activity raises issues of privacy as it allows those with control over communications systems to build up a profile of the user and target them for commercial purposes, criminal investigation or other reasons. Although records and logs are a natural by-product of advanced telecommunications systems – billing and systems maintenance are standard beneficiaries of this data retention – the information that is retained and its possible transfer to a third party requires regulation to ensure users' privacy is protected. The ICCL is concerned that the development of various databases by state and non-state actors – of which this is but one – could lead to a culture of "Dataveillance" i.e. surveillance through the use of databases. In this respect, it is essential that the data retained under provisions in the Bill is used for those specified purposes only.

This submission assesses four areas of the Bill where the ICCL considers that privacy rights may be most at risk: blanket retention; retention periods; disclosure of data; and, oversight and remedy. In the analysis, particular reference is made to Article 8 (right to private life) of the ECHR. Further effect was given to the ECHR in Irish law under the European Convention on Human Rights Act 2003.

---

[1] Hereinafter referred to as "the Bill".

[2] Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC; hereinafter referred to as "the Data Retention Directive".

[3] Article 1.

[4] *Klass v Germany* (1978) 2 E.H.R.R. 214; *Malone v UK* (1985) 13 E.H.R.R. 448 and (1985) 7 E.H.R.R. 14; *Huvig v France* (1990) 12 E.H.R.R. 528; *Halford v UK* (1997) 24 E.H.R.R. 523; *A,B,C,D v Germany*, App No. 8290/78; 18 D.*R; TS and FS v Italy* App.No. 13274/87; 66 D.R.

[5] There is no express right to privacy under the Irish Constitution; however, it has been recognised as a fundamental right by the courts. Many facets to private life exist and several articles in the Constitution provide protection for privacy, including, Article 40.1.3 (personal rights), Article 40.5 (inviolability of the dwelling), Article 41 (rights of the family) and Article 43 (private property rights). See, for example, *Kennedy v. Ireland*, [1987] IR 587; *McGee v. Attorney General* [1974] IR 284; *Hanahoe v. Hussey* [1998] 3 IR 69; *Ryan v. Attorney General* [1965] IR 294; *I. O'T v. B* [1998] 2 IR 321; *Cogley v. Radio Teilifís Éireann* [2005] 4 IR 79; *Gray v. Minister for Justice* [2007] 2 IR 654.

The requirement to respect private life under the Convention is wide-ranging and in determining its scope, the European Court of Human Rights considers the notions of personal autonomy, human dignity and freedom which underlie Article 8.[6] Although the right to privacy under Article 8 is not absolute or guaranteed in all circumstances,[7] interferences with the private life of an individual may be allowed only if they can be shown to be lawful and necessary in a democratic society and for certain specified reasons (including national security and the prevention of crime or disorder). Even if an interference can be shown to be lawful and necessary in a democratic society, it must also be proportionate to the pursuit of a legitimate aim. This is discussed further below.

The ICCL considers that the right to privacy must remain central to all relevant policy and law making development. In this respect, the ICCL agrees with the following statement of the Law Reform Commission:

> Privacy is not merely instrumental to the achievement of other goals but is a basic human right that applies to all persons by virtue of their status as human beings. It is not possible to overstate just how fundamental privacy is in a civilised legal system".[8]

[6] *Pretty v. United Kingdom* (2002) 35 EHRR 1.

[7] The right to privacy is a "qualified" right under the ECHR and international human rights law such as Article 17 of the International Covenant on Civil and Political Rights. This means that the right to privacy can be curtailed for specified reasons.

[8] Law Reform Commission, *Privacy, Surveillance, and the Interception of Telecommunications*, LRC (57-1998), p. 2.

2. Blanket Retention

As set out in the Data Retention Directive, the retention regime proposed in the Bill incorporates a system of blanket data retention. In practice, the measures would entail ongoing monitoring of the data used by the population and the use of pre-emptive surveillance.[9] The ICCL is concerned that the Data Retention Directive and any implementing legislation could contravene Article 8 (right to private life) of the ECHR.

At present, Part VII of the Criminal Justice (Terrorist Offences) Act 2005[10] sets out the legal basis for the retention of telephone data (mobile and fixed line) in Ireland. However, internet usage is currently not monitored or retained. Part VII will be repealed by Bill[11] which will subsequently provide for the retention of both telephone and internet usage. In line with the current measures in the 2005 Act, the Bill will cover both call logs and location information; however, it will not apply to the *content* of the communications.[12] Notwithstanding this, it has been reported that the Garda Commissioner has written to telecommunications providers requesting that web-browsing information, including the content of web-based email be retained, on the basis of "good citizenship" and assistance to criminal investigations.[13] Such activities would have worrying privacy implications and the lack of legal basis for such data content retention may fall foul of Article 8 (right to private life) of the ECHR.

In the case of *Liberty, the Irish Council for Civil Liberties and British Irish Rights Watch v. The United Kingdom*,[14] the European Court of Human Rights found that the rules governing data interception and retention in the United Kingdom did not "set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material". Therefore, the interception and retention over a seven year period, of all telephone, fax, e-mail and data communications between the UK and Ireland, was a disproportionate interference with the applicants' rights under Article 8 and a violation of the Convention.

In *S. and Marper v. UK*,[15] decided in 2008, the Court scrutinised English and Welsh laws on the indefinite retention of DNA samples taken from any person arrested for a recordable offence. This challenge was taken by 'S' who was 12 when he was charged with attempted robbery in 2001 but later cleared. Michael Marper, also a party to the case, was charged with harassing his partner in 2001 but the case was later dropped when they reconciled. Both men subsequently asked for their fingerprints and DNA profiles to be destroyed but South Yorkshire police refused and stated the samples would be retained "to aid criminal investigation".

---

[9] McIntyre, T.J., "Violations only made worse by new plans for data retention", *Irish Times*, 4 June 2008.
[10] Hereinafter referred to as the "2005 Act".
[11] S. 13.
[12] S. 2.
[13] Lillington, Karen, "Garda Chief asks mobile phone firm to retain web-browsing data", *Irish Times*, 7 November 2008.
[14] Application no. 582443/00, 1 July 2008.
[15] Application nos. 30562/04 and 30566/04, 4 December 2008.

The European Court of Human Rights rejected the claim that sweeping up the innocent with the guilty is necessary to fight crime. The Court was also struck by the "blanket and indiscriminate nature" of the power of retention in England and Wales and compared it with Scotland, where samples are retained from suspects for three years but only in relation to violent or sexual offences.[16] Taking into account the Court's focus on necessity and proportionality as evidenced in the *S and Marper* case, it is possible that the data retention framework proposed under the Bill may not be justifiable under Article 8 due to its broad and indiscriminate nature.

Although laid down in the Data Retention Directive, the ICCL is not convinced that the all-encompassing system of data retention proposed in the Bill is compatible with the right to private life under the ECHR. In this respect, the ICCL notes that successful legal challenges have been taken against blanket data retention across a number of European states including Germany.[17]

ICCL Recommendation:
Telecommunications and phone records should be retained only where there is a legitimate suspicion that a serious offence has been committed rather than in the blanket manner proposed in the Bill.

[16] *Op cit*, para 119 and 109.
[17] For more on this, see www.digitalrights.ie [accessed 10/11/09].

3. Retention Periods

The Data Retention Directive stipulates that communications data should be retained for at least six months and no more than two years.[18] However, the Bill imposes an obligation on service providers to retain telephone data for a period of two years and internet data for one year.[19] Therefore, the period of data retention that the Government proposes to introduce in Ireland is at the very top end as compared to our European counterparts e.g. in the UK the retention period for both telephone and internet records is 12 months.[20]

Under the Data Protection Acts 1988 and 2003, personal data should not be kept for longer than is necessary for the purpose intended.[21] In this respect, the application of the uppermost time limit in the Bill seems excessive and at odds with the general protections for data under data protection law.

The European Court of Human Rights gives further guidance on the retention of personal information for longer than is necessary. In *Amann v. Switzerland*, the Court found that the storing of information in relation to an individual's private life by the state amounted to an interference with that private life. In this case, the Court held that the Swiss authorities should have destroyed the stored information "when it emerged that no offence was being prepared".[22] As mentioned, under Article 8 (right to private life) of the ECHR, any interference must be "necessary in a democratic society". It must also be proportionate to a legitimate aim. If the legitimate aim - under the Bill, the prevention of crime or disorder and national security considerations - could be achieved using less restrictive means, it is possible that excessive actions may constitute a violation of Article 8.[23] This begs the question therefore, is it necessary that telephone data be retained for two years or can the same result be achieved using less restrictive means, for example 12 month retention periods?

A further issue which is connected strongly to the length of retention is that of data security. Following numerous data breaches[24] and the absence of a breach disclosure law within current data protection laws, how can the public be assured that private communications companies will keep the data safe? Shorter periods of retention may help to reduce the risk that security will be compromised. Notwithstanding that, at all times, the companies concerned should be required to have robust security measures in place.

---

[18] This is substantially less than the 3 years for which phone records are currently retained under s. 63 of the Criminal Justice (Terrorist Offences) Act 2005.
[19] S. 3.
[20] Data Retention (EC Directive) Regulations 2009 (SI/2009/859), s. 5.
[21] S. 2.
[22] *Amann v. Switzerland,* (2000) 30 E.H.R.R. 843, at para 78.
[23] A restriction could not be "necessary in a democratic society" unless to was "proportionate to the legitimate aim pursued", *Handyside v. UK* (1979-1980) 1 EHRR 38 at para 49.
[24] See, for example, Breda Heffernan and Edel Kennedy, "Alert as 170,000 blood donor files stolen", *Irish Independent*, 20 February 2008; "Staff details on latest missing State laptop", *Irish Examiner*, 2 August 2008; "BOI faces possible €100K fine and claims over stolen laptops", *Irish Examiner*, 23 April 2008; David Labanyi, "Commissioner investigating loss of bank customers' details", *Irish Times*, 5 November 2008; and Elaine Edwards and Pamela Newenham, "Laptop with HSE staff details stolen", *Irish Times*, 11 September 2008.

ICCL Recommendation:

- **Retention periods should be reduced to six months for all communications data - both telephone and internet - in line with the proportionality principles of the European Convention on Human Rights.**

4. Disclosure of Data

The Bill enables the Gardaí, members of the Defence Forces and revenue officials to make a disclosure request to access retained data.[25] This is an extension of the powers that were available under the Criminal Justice (Terrorist Offences) Act 2005, under which only the Gardaí and the Defence Forces could request the data.

Generally requests must be made in writing. However, the requirement that data requests be made in writing may be dispensed with in times of urgency and a request can be made orally.[26] When oral requests are made, these should be followed up in writing within 2 days of such request.[27] However, it is unclear what safeguards are proposed for the making of oral requests. How can a service provider verify that the person making the request has the authority to do so, particularly if such a request is not made in person? This is particularly relevant given that provisions of the Bill oblige a service provider to comply with such data requests.[28]

While the Gardaí and Defence personnel deal with law enforcement and security measures, revenue officials are concerned with specific "revenue offences", defined in the Bill as excise offences; tax fraud; oil smuggling; non payment of excise duties; and smuggling of tobacco or alcohol.[29] However, these activities are all indictable offences and accordingly, the relevant data requests could easily come within the remit of the Gardaí. The ICCL is concerned that the empowerment of revenue officials to access personal data is not a proportionate response to revenue collection difficulties. This is compounded by the absence of a requirement for judicial or other authorisation before the disclosure request can be made. In this respect, the ICCL refers to the European Commission report on the transposition of the Data Retention Directive[30] which outlines the access conditions applicable to state agents who request communications data. The measures used vary across the different countries; however, few are as lax as the system proposed under the Bill. In many, a court order or the approval of a judicial actor is required. To ensure adequate protection for the right to privacy, the ICCL considers that judicial approval should be required before a data access request can be made.

ICCL Recommendations:

- **Only Gardaí and Defence Forces personnel should be authorised to access to communications data;**
- **Data requests should be subject to judicial approval.**

[25] S.6.
[26] S. 6(4).
[27] S. 6(5).
[28] S. 7.
[29] S. 1.
[30] European Commission, Transposition of Directive 200/24/EC (Data Retention) by EU Member States and EFTA (further to oral reports at the meeting of 22 January 2009 in Brussels).

5. Oversight and Remedy

Oversight

Under the current system, a designated High Court judge reviews the operation of the 2005 Act and determines whether the Gardaí and the Defence Forces are complying with the provisions.[31] Similar to this procedure, the Bill provides for review by a sitting High Court judge as appointed by the Minister for Justice, Equality and Law Reform. The judge would be required under the Bill to provide periodic reports to the Taoiseach on the operation of the Act.[32]

The ICCL considers that the monitoring mechanisms proposed are lightweight as compared to the nature of the data retained, the period for which it is retained and availability of access to revenue officials as well as security and crime personnel. The adequacy of oversight procedures should be considered in the context of recent criticism of the current regime of judicial oversight under the 2005 Act (and in relation to the interception of communications, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993). The present reporting format consists of a one page document containing a single paragraph stating that records in relation to the Acts had been examined by the judge.[33] The ICCL considers that this raises serious questions in relation to transparency.

Furthermore, the statistics prepared by the Garda Commissioner, the Chief of Staff of the Permanent Defence Forces and the Revenue Commissioners are submitted to the relevant Ministers only.[34] Again for reasons of accountability and transparency, the ICCL considers that the statistical reports should be laid before the House of the Oireachtas also.

The European Court of Human Rights has pointed out that, in light of the risk that a system of secret surveillance for the protection of national security can pose of "undermining or even destroying democracy on the ground of defending it", there must be adequate and effective safeguards in place to protect against abuse.[35]

Remedy

There is a complaints procedure set out in the Bill which includes the appointment of a referee.[36]

---

[31] S. 67. Under ss. 66 and 67, the judge has the power to investigate any case in which disclosure is made and to inspect any official documents or records relating to the request.

[32] S. 12(1) (b). The reports will be laid before the Oireachtas but the Taoiseach can exclude material for security reasons. Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, s. 8(6).

[33] See Mark Tighe, "Judges' Phone Tap Report 'is laughable'", *Sunday Times*, 23 May 2009. A copy of the report is available on http://tjmcintyre.com [accessed 10/11/09] under "Transparency in overseeing state surveillance: How not to do it", 15 May 2009.

[34] S. 9.

[35] *Leander v. Sweden* (1988) 9 EHRR 433, at para 60. In this case the Swedish government were found to have sufficient safeguards in place. See *Rotaru v. Romania*, Application no. 28341/95, 4 May 2000 where the Court stated "judicial control affords the best guarantees of independence, impartiality and a proper procedure", at para. 59.

[36] S. 10.

However, where correct procedures surrounding the request for disclosure have not been followed by the Gardaí, Defence personnel or revenue officials, the disclosure request will not invalidated and the person whose privacy has been infringed will have no cause of action. A contravention of procedures could take the form of something as seemingly innocuous as a delay in following an oral request with a written request; however, it could concern a more serious matter and this should not be discounted.

Moreover, where the basis of a data request was unfounded, the reputation of an innocent individual could be unduly brought into disrepute and could lead to defamation of the individual concerned.

In the case of *Perry v. United Kingdom*, the European Court of Human Rights held that police officers who did not abide by the procedures set down in law for the taking of video footage interfered with the privacy of the individual concerned. The Court reached this conclusion because the images generated by the video could not be considered to be "in accordance with law" as set out in Article 8 (right to private life) of the ECHR.[37] Furthermore, the Court has found that "any individual measure of surveillance has to comply with the strict conditions and procedures laid down in the legislation itself".[38] This raises doubts regarding the assertion in the Bill[39] that a disclosure request that was not carried out in accordance with the procedures will not be rendered invalid as a result.

ICCL Recommendations:

- **Comprehensive reporting mechanisms should be obligatory under the Bill as part of the independent judicial oversight framework;**
- **For reasons of accountability and transparency, the statistical reports submitted by the Garda Commissioner, the Chief of Staff of the Permanent Defence Forces and the Revenue Commissioners for the relevant Ministers should be laid before the House of the Oireachtas;**
- **Appropriate remedies should be available under the Bill for individuals whose privacy was compromised by unauthorised or unfounded disclosure requests.**

[37] *Perry v. United Kingdom*, Application no. 63737/00, 17 July 2003.
[38] *Klass v. Germany*, *op cit*, at para 43.
[39] S. 10(1).

6. Conclusion

Internet and phone records can provide valuable information to aid the investigation of offences; however, access to this information must be achieved through the least intrusive means possible. Data retention carries with it financial implications and administrative burdens which do not seem to have been considered in relation to the data retention regime proposed under the Bill. Furthermore, it has been reported that a substantial number of Irish email accounts will fall outside the scope of the Bill as many service providers are not based in Ireland.[40]

Most importantly, the broad retention of data as suggested under the Bill designates "a shift in the balance between the citizen and the state that may be presumed to be irreversible: surveillance powers, once granted, are rarely rolled back".[41] In this respect, the ICCL awaits with interest the outcome of the case lodged by *Digital Rights Ireland*[42] with the Irish High Court challenging the validity of the Data Retention Directive on the basis that it breaches the right to privacy as laid out in Article 8 (right to private life) of the ECHR (among other issues). In July 2008, the Human Rights Commission received leave from the High Court to appear before the Court in this case as *amicus curiae*.[43] The conclusion of this case should provide an important indicator of the extent to which governments can retain data on individuals and remain compliant with Article 8 (right to private life) of the ECHR.[44]

The ICCL considers that it is essential that we maintain the highest possible protection within our legal system for the right to privacy. The right to privacy underpins the principles of freedom and liberty which form the core of a democratic society. Advancements in technology should be harnessed to promote and defend democracy, not deployed to limit our fundamental rights. To this end, the ICCL believes that the right to privacy should be at the heart of any deliberations on the Bill.

[40] "Web-based mail exempt from data retention", *The Sunday Business Post*, 19 July 2009.
[41] www.digitalrights.ie [accessed 10/11/09].
[42] See www.digitalrights.ie.
[43] Meaning 'friend of the court', the Irish Human Rights Commission will make submissions on the human rights dimensions of the case.
[44] For comprehensive coverage of the data retention debate and ongoing updates see www.digitalrights.ie.