We Know What You Did Last Summer!

What aims should guide Ireland's laws on data retention?
Review current proposals in the light of those aims?

Alan Woods

"Laws are the conditions under which men, naturally independent, united themselves in society. Weary of living in a continual state of war, and of enjoying a liberty which became of little value, from the uncertainty of its duration, they sacrificed one part of it, to enjoy the rest in peace and security."

-Cesare Beccaria[1]

Each and every day, Irish citizens during the course of their daily routines on some level, either consciously or not, obey the law; a small fraction of these citizens do not. For the protection of our way of life we empower certain members of society to prevent the breaking of the law. To these few protectors, society imparts powers and privileges to investigate, find and bring the perpetrators of crime to justice. However in the conferring of these powers and functions, society must make a choice: How much privacy and autonomy must be sacrificed for the prevention of crime?

The focus of this paper is one such incursion into the rights and freedoms of citizens in the name of security, that of Traffic Data Retention (hereafter 'TDR'). The concept of TDR is that every phone, mobile and Internet service provider compiles and retains records of all traffic data on their systems; essentially who called who, and when the call took place; in the case of mobile phones where the caller was and in the case of web browsing, a list of sites that were visited and to whom e-mails were sent and from whom they were received. The data is to be retained for a set minimum time period and would be made available for perusal by the authorities in the process of investigating a crime. Undoubtedly such a compilation of 'personal'[2] data comes with intricate privacy and cost complications and thus has been the source of much heated and heavy debate.

This paper will be divided into 3 sections

1) This section will investigate the roots of TDR and will attempt to map the reasons why such new and radical measures are proposed.
2) Section 2 will give a brief overview of the European policies and approaches to the topical question of TDR
3) Finally, section 3 will assess the Irish Proposals on Data Retention and, in light of international example consider whether or not the Irish aims are being met in the best way possible.

Section 1 – Aims of TDR

9/11:- Panic and Mitigation

[1] C. Beccaria, *Dei delitti e delle pene: An Essay on Crimes and Punishment*, 1764, I

[2] Some of the data is not *per se* personal as it is non-traceable to individual users eg. Anonymous e-mail addresses, however, as will be investigated later in the paper, a vast portion of the retained data may very well be considered Personal Data.

> "The Terror attacks of September 11, 2001 did not usher in a new era but serve as a stark reminder of the globalization of terrorist and criminal threats to public safety"[3]

With the fall of the twin towers, so too fell the strength of privacy rights worldwide. Although the US government continued to call for a balanced approach to TDR, an approach that would strike a balance between the protection of personal privacy and public safety[4], the intense flurry of anti-terrorism sentiment that followed in the wake of 9/11 seemed to alter the world's perception of the word 'balance'. Although mandatory data retention had been called for, for many years previous to 9/11, it was on the 20th of September 2001, 9 days after the terror attacks, that the EU Justice and Home Affairs Council put it to the top of the agenda as one of the measures to combat terrorism. On the 12th of July 2002, the EU agreed to a basic and fundamental change to the 1997 Directive on privacy and telecommunications. [5] According to Privacy International, in every country that changed its laws in reaction to 9/11, provision was made for an increased ability of law enforcement and national security agencies to intercept communications.[6]

Indeed the concept of telecommunications surveillance is not a new measure. Surveillance has been carried out on a global scale by the world's intelligence agencies prior to 9/11. The National Security Agency (US) and the Government Communications Headquarters (GCHQ, UK) have carried out surveillance of world communications since 1947[7] under the UKUSA agreement. During the cold war, systems such as ECHELON targeted political and economic intelligence, and most recently the NSA has created it's huge online storage system known as Petraplex designed to hold all the world's communications for a period of 90 days. Although the power of telecommunications surveillance was normally given to intelligence agencies, law enforcement agencies apparently harboured the wish to gain access to traffic and location data. Michael McDowell, the Minister for Justice, Equality and Law Reform, announcing the consultation process to introduce TDR in Ireland, justified it as being "necessary " in the fight against crime[8]. While it is reasonable to accept that the EU's law enforcement agencies' demand for the retention of data, has little or nothing to do with the prevention of terrorism but seeks to deal with crime and international threats posed by public order, refugees and asylum-seekers undoubtedly world events have aided in the fulfilment of this wish. [9]

The Importance of TDR to Law Enforcement

---

[3] From the *Prepared statement of the United States of America,* Presented at the EU Forum on Cybercrime, Brussels, 27 November 2001 (presented by Mark Richard, Criminal Division of the United States Department of Justice)

[4] ibid

[5] DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

[6] Privacy International, *Privacy and Human Rights 2003: Threats to Privacy*, Http://www.privacyinternational.org/survey/phr2003/threats.htm at p.3

[7] See Statewatch News Online, *Majority of Governments introducing data retention of communication,* , http://www.statewatch.org/news/2003/jan/12eudatret.htm , January 2003.

[8] M. McDowell, *Press Release "McDowell launches online consultation on data retention",* Dept. of Justice, 21st March 2003, Http://www.justice.ie/802569B20047F907/vWeb/pcCAMC5LFDNB (last visited 26/03/04)

[9] ibid.

Before the concept of TDR can be hailed as an unacceptable invasion of privacy, the question must be asked: can it be justified? According to the *APIG report* [10], "there is considerable evidence that communications data relating to telephone usage (both fixed and mobile) is of great importance to Law Enforcement Agencies."[11] Here in Ireland, according to Assistant Garda Commissioner Joseph Egan, speaking at The Department of Justice Consultation Forum on Data Retention, 24th February 2003, the use of telecommunications data has been "central" in the bringing of prosecutions in the murder of Veronica Guerin and of those responsible for the Omagh Bombings. He continued on to state that data retention was "a huge requirement" for Gardaí and criminal investigations would be "very much hindered" without adequate provisions for the retaining of traffic data.[12]

Section 2 : European Policy

European 'About Face'

On the 20th May 2002, the European Parliament, in what has been called a "remarkable reversal of their original position"[13] voted on the European Union Electronic Communications and Privacy Directive[14] (hereafter 'the directive'). Reversing the 1997 Directive[15], the directive under Art. 15 (1) now explicitly allows European Union Countries to "compel Internet service providers and telecommunications companies to record, index, and store their subscribers' communications data"[16]. Luckily the directive does not cover the contents of communications.

In the wake of this new Directive sanctioned 'carte blanche', Member States have been very busy in preparation of their own laws on mandatory data retention. This section will endeavour to chart briefly the effect of the Directive in the member States with a specific focus on our closest European Neighbour, the UK.

European Overview

In January 2003, Statewatch[17] carried out a survey on the various data retention laws applicable or pending within the Member States of the European Union. In its conclusions, it found that 9 of the 15 EU States had or have the intention to introduce an obligation for the retention of data. The survey also showed that only two Member States had no plans to implement a mandatory policy and 4 were undecided as to their course of action. Countries with definite plans included Greece who felt "the creation of such a legal tool [as mandatory data retention] to be important useful and essential.".[18] Italy under their law no. 171 of 13/5/1998 does not allow the retention of data for purposes other than for billing but have proposed a

---

[10] supra fn. 15 at p. 3 para. 8
[11] ibid. at p. 3
[12] K. Lillington, *State secretly retaining phone data*, Irish Times 25/02/03
[13] supra fn 6 at p.20
[14] Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the Electronic Communications sector (Directive on Privacy and Electronic Communications)
[15] Supra fn. 5
[16] supra fn. 6 at p. 20
[17] Supra fn. 7 at p. 3
[18] ibid.

review as "this lack of precious information in support of criminal investigations could pose serious obstacles"[19]. Luxembourg was found to be drafting a law to incorporate the changes in the directive, as too were Portugal, Spain and the Netherlands. Ireland, as will be discussed in section 3, is shown to be planning a law on the matter, however the survey noted that the Irish proposal for a 3-year retention period far out reached any other Member State's domestic provisions.

UK:- RIP to Communication Privacy

The UK first found the power of data retention under the Regulation of Investigatory Powers Act 2000 (hereafter 'RIPA'). S. 22 (2) of the RIPA sets out the process for which access may be given to all types of communication data, broadly encompassing national security, public safety and the economic well being of the state. According to *Akdeniz, Walker & Taylor* the RIPA "encouraged by European Union edicts,... potentially empowers an alarmingly large range of public agencies to snoop, ranging from the Egg Inspectorate to GCHQ, and for a rambling array of reasons.". Opposition to these provisions is quite apparent in both academic and legal circles, the UK Data Protection Commissioner himself being critical, contending that "access to traffic and billing data should also be made subject to prior judicial scrutiny".[20]

In the wake of 9/11, the UK passed the Anti-Terrorism, Crime and Security Act 2001 (ATCS). Sections 102 to 107 of the Act make arrangements for companies to store communications data in order for the police to be able to trawl it. Thus, who you email, who you phone, what websites you visit, what information you give to those websites, what files you download, who phones you and who emails you would be retained and made available for the police investigating any offence. The main clause under s.102 involves voluntary codes of practice, but s.104 enables the Home Secretary to require that a communications service provider retain the data mandatorily. Although this power is limited to the time limit of 2 years, the Act makes a further provision for the renewal of this time limit under s.105 (3). According to the *Communications Data: Report of an Inquiry by the All Party Internet Group*, the intention of the ATCS legislation was to ensure that communications data would be available for Law Enforcement to access for a substantial period.[21]

On review of the provisions of the RIPA and the ATCS, the All Party Internet Group, expressed that great fault was found with the data retention schemes. They concluded that the regime envisaged would be immensely expensive[22] and left the group with significant doubts as to its lawfulness. APIG believed that mandatory data retention would do immense harm to the communications service provider industry and that fundamentally it was just not practical "to retain all communications data on the off chance that it will be useful one day." The ultimate recommendation of the

---

[19] ibid.

[20] Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] *Criminal Law Review*, (February), pp. 73-90. at p.81

[21] *Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003,* Http://www.apig.org.uk at p.22 para. 129

[22] Even with the government assistance on costs, which would amount to £20 Million. The Actual costs were estimated by the report (at p.22 para 145) that the actual costs of the mandatory regime to be in excess of £100 million.

report was that the government should **not** invoke the powers under s.104 of the act in the imposition of a mandatory data retention scheme. [23]

Interestingly in transposing the Directive[24] by means of Statutory Instrument 2426 of 2003[25], there is no mention under regulation 7[26] of mandatory TDR. Although the RIPA and ATCS are not mentioned in the regulations, thus making it apparent that the powers under s.104 of the ATCS are still available to the British Government.

European Uncertainty:- Time and Second Thoughts

In reaction to the terrorist attacks of 9/11, the EU reacted in an unmistakably hasty manner to a new and seemingly powerful threat. Borne from this haste, it would appear that a Procrustean bed was created, one that stretched the limits of freedom to fit the demands of government officials gripped with fear and uncertainty. With the European change of heart with regards to TDR, many countries the UK to the fore, felt it necessary to introduce draconian measures in the name of national security and crime prevention. As is apparent from reports such as the APIG report, hindsight and time has eased the mania surrounding the power of terrorism and recommendations show that, when approaching the concept of TDR, such reports, while recognising its use, see the need for a balanced approach.

Section 3: Ireland's Aims and Policies

The Right to Privacy

Ireland, although not having an express right to privacy in the Constitution, finds an unenumerated protection under Art. 40.3.1 and its interpretation in *McGee v. A.G.*.[27], which recognised the right to marital privacy. This was followed and extended by the decision in *Kennedy & Arnold v. Ireland*[28], where the Supreme Court ruled that the illegal wiretapping of two journalist's phones was a violation of the constitution, stating:

> "The right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State… The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society. This cannot be insured if his private communications, whether written or telephonic, are deliberately and unjustifiably interfered with."
>
> Needless to say the right to privacy is hugely important and the courts have been consistent in its protection. TDR, when limited, is acceptable. However if these limits are exceeded, at what point will such an incursion become a violation to our right to privacy? Hope would reason that our Government would take such important issues into account when legislating for it's people,

[23] Supra fn. 15 at p. 27 para 176-178
[24] Supra fn. 14
[25] 2003 No. 2426, ELECTRONIC COMMUNICATIONS, The Privacy and Electronic Communications (EC Directive) Regulations 2003
[26] Which deals with the restrictions of traffic data retention.
[27] [1974] I.R. 284
[28] [1987] I.R. 587.

however, it would appear that the Supreme Court and The Government do not live by the same standards.

Data Retention: Irish Style

On the25th February, 2003, Karen Lillington of the Irish Times reported that the government had "had a secret data retention regime for almost a year, after the Cabinet confidentially instructed telecommunications operators to store traffic information about every phone, fax and mobile call for three years", she continued on to State that the Data Protection Commissioner, Joe Meade, revealed that ex- Public Enterprise Minister, Mary O'Rourke had issued secret directions for data retention when a dispute arose between operators as to how long data should be stored.[29] Mr. Meade, has also threatened High Court Action against the government in light of these revelations[30]. It should be noted that the Irish Government had also, in response to European Questioning in 2002, admitted in a leaked document that Primary Legislation was being prepared, that included a proposed 3 year time period, for TDR[31]. It was not until a year later that the Minister for Justice announced a consultation process on a new Data Retention Bill[32].

As for the justification for such Provisions, the above leaked Questionnaire stated that

> " The proposed primary legislation on the retention of traffic data will provide for compliance with any request from the police (Garda Síochána) or the Defense Forces for disclosure of data, in the interests of the prevention and investigation of serious crime, in the interests of national security and in the discharge by Ireland of its international obligations relating to terrorism."[33]

This stance is not surprising and can easily be found to be in line with the common European 'way' of thinking. With nothing but proposals floating, one can only surmise as to what will be included in the Bill, or even its first draft. No such draft legislation has yet appeared, although such a draft bill was promised last autumn.[34]

3 Years:- "Way Out Ahead" of Everyone Else

Although the proposals for the mandatory retention of traffic data are enough in their own right to cause controversy and argument, a more serious criticism is the proposal for a 3-year retention period. This period has been recognised by the Statewatch Survey to be "way out ahead" of the rest of Europe, with the normal

---

[29] Supra fn. 12
[30] see K. Lillington, *Court threat for State over data privacy,* Irish Times, May 26, 2003
[31] Document entitled:
Following the dispatching of a questionnaire on traffic data retention (Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1) that was directed at the Multidisciplinary Group on Organised Crime (MDG), the General Secretariat now presents in the annex the comprehensive answers that have been submitted by Member States' delegations.
Available on http://www.effi.org/sananvapaus/eu-2002-11-20.html
[32] Supra fn. 8
[33] Supra fn. 31 at Question 3
[34] K. Lillington, *Departments at odds on Data Retention Bill,* Irish Times, June 27 ,2003

period for TDR being set at 12 months.[35] Four of the world's largest business and technology industry groups[36] have issued statements to the effect that government proposals for TDR were for "excessive periods". Questioned about this, Minister McDowell replied that "The time limit being considered is three years which is shorter than the period which licensed operators historically retained such information for billing purposes.". This is indeed true to a point as Vodafone and Eircom did indeed retain traffic data for billing purposes for a period of 6 years, however following complaints to the Data Protection Commissioner, this was quickly reduced to 6 months[37]. The Minister was undoubtedly aware of this fact.[38]

Mandatory TDR:- Costs and Feasibility

As noted by the *APIG* report in relation to s. 104 of the ATCS, the costs of a mandatory retention of all traffic data, economically speaking is just not feasible. In the UK alone, AOL estimated that such retention of data from their Internet Service would fill 360,000 CDs each year and cost an estimated £34Str[39] . The Irish Department of Communications have themselves voiced their concern at the costs that would be incurred at the expense of the telecommunication companies and service providers, stating that it:

> "Would impose significant initial capital expenditure costs on operators as well as ongoing expenditure related to operational requirements. This would probably be an additional deterrent to market entry by new service providers. It must also be assumed that additional costs for industry will result in increased costs for subscribers and users".[40]

CONCLUSION

Nearly 3 years after the dust clouds of 9/11 have settled, It would appear that the initial panic that ensued worldwide about security and in particular the monitoring of telecommunications has been recognised to be alarmist. While the European union has allowed mandatory TDR to be carried out, with the Majority of Members States having opted to do so, a level of common sense is being applied.[41] Unfortunately the Irish position has apparently missed out on the common sense approach and has rushed headlong into controversy. If the aims of data retention were the prevention and investigation of crime, national security and the protection of the economic well being of the country, then it would appear that the Department of Justice have missed its point completely. With elevated costs, Ireland would cease to be a competitive e-

---

[35] Supra fn. 7 at p. 7

[36] The four groups include the International Chamber of Commerce Commerce (ICC), the Union of Industrial and Employers' Confederations of Europe (UNICE), the European Information, Communications and Consumer Electronics Technology Industry Association (EICTA) and the International Telecommunications Users Group (INTUG).

[37] The Data Protection Act 1998, s. 2(1)(C)(iv) states that in relation to the retention of data such as traffic data " the data shall not be kept for longer than is necessary for that purpose or those purposes"

[38] K. Lillington, *Don't believe State on data retention,* Irish Times, 14th March 2003.

[39] BBC News Online, *UK Stands Firm on Snooping Laws,* January 30, 2003, Http://www.bbc.co.uk/1/law/technology/2706677.stml

[40] Supra fn. 34

[41] This can be see from the British Government's apparent reluctance to invoke s.104 of the ATCS

commerce force and with a 3-year data retention period the Irish people would find themselves subject to an unbalanced and unwarranted incursion on the right to privacy. Maybe in the aftermath of 9/11 such measures may have seemed warranted; the world's dignity was attacked and the Western Governments reacted hastily and harshly. Where as time has calmed excessive fears in other countries, so that more draconian provisions are left in abeyance,, Ireland seems to be trudging on even if our society and its freedom is ultimately compromised.

"Others have estimated crimes rather by the dignity of the person offended than by their consequences to society."

\- Cesare Beccaria[42]

Bibliography

LEGISLATION

- DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

- Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the Electronic Communications sector (Directive on Privacy and Electronic Communications)

- (UK) S.I. 2003 No. 2426, ELECTRONIC COMMUNICATIONS, The Privacy and Electronic Communications (EC Directive) Regulations 2003

- The Data Protection Act 1998

Other Sources

- C. Beccaria, *Dei delitti e delle pene: An Essay on Crimes and Punishment*, 1764

- *Prepared statement of the United States of America,* Presented at the EU Forum on Cybercrime, Brussels, 27 November 2001

- Privacy International, *Privacy and Human Rights 2003: Threats to Privacy*, Http://www.privacyinternational.org/survey/phr2003/threats.htm

- Statewatch News Online, *Majority of Governments introducing data retention of communication, ,* http://www.statewatch.org/news/2003/jan/12eudatret.htm , January 2003.

- M. McDowell, *Press Release "McDowell launches online consultation on data retention",* Dept. of Justice, 21st March 2003,

[42] Supra fn.1 at VII

Http://www.justice.ie/802569B20047F907/vWeb/pcCAMC5LFDNB (last visited 26/03/04)

- K. Lillington, *State secretly retaining phone data*, Irish Times 25/02/03

- Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights,
  [2001] *Criminal Law Review*, (February), pp. 73-90. at p.81

- *Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003,* Http://www.apig.org.uk

- *McGee v. A.G* [1974] I.R. 284

- *Kennedy & Arnold v. Ireland* [1987] I.R. 587

- K. Lillington, *Court threat for State over data privacy,* Irish Times, May 26, 2003

- Document entitled:
  Following the dispatching of a questionnaire on traffic data retention (Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1) that was directed at the Multidisciplinary Group on Organised Crime (MDG), the General Secretariat now presents in the annex the comprehensive answers that have been submitted by Member States' delegations.
  Available on http://www.effi.org/sananvapaus/eu-2002-11-20.html

- K. Lillington, *Departments at odds on Data Retention Bill,* Irish Times, June 27 ,2003

- K. Lillington, *Don't believe State on data retention,* Irish Times, 14th March 2003.

- BBC News Online, *UK Stands Firm on Snooping Laws,* January 30, 2003, Http://www.bbc.co.uk/1/law/technology/2706677.stml