"Legal protection of information privacy … can be linked to a privacy patchwork quilt with quite a few holes in it"[1]

An analysis of the Irish Data Protection law in relation to the protection of privacy in the online environment

by Máiread Cronin

[1] Dworkin, "Privacy and the Law" in Yong (ed.), Privacy (John Wiley & Sons, 1978) 113.

It is proposed to show in the course of this essay how this quotation aptly describes the protection provided by the Data Protection Act, 1998[2] to privacy in the online environment. In Ireland, the concept of privacy has been fused with the data protection which interprets privacy in terms of management of personal information.

"The Internet is a network of computers communication with each other on the bases of the Transport Control Protocol/Internet Protocol (TCP/IP). It is international network of interconnected computers, which enables millions of people to communicate with one another in 'cyberspace' and to access vast amounts of information from around the world."[3] The concept of sharing and receiving information is central to the ethos of the Internet. However, the openness of the Internet means it is very susceptible to the gathering of personal information by surreptitious and transparent means, often without individuals consent. Personal information is converted by several actors of the Internet eg. Governments who wish to tackle cyber crime, and companies who by receiving personal profiles of customers may identify target audiences for its goods, and engage in direct marketing. The effectiveness of data gathering technologies in invading privacy will be determined by the effectiveness of data gathering technologies in invading privacy will be determined by "the reason for which they are deployed on particular occasions, by the regulatory framework and security arrangements that surround their use, and by the capacity of individuals to take steps to prevent

[2] Hereinafter referred to as the DPA

[3] Article 29 Working Party Working Document, Privacy on the Internet – An Integrated EU Approach to Online Data Protection adopted November 2000, and pg.8. Hereinafter referred to as Privacy on the Internet.

the unauthorised collection and use of their personal information."[4] This means that legislation alone is not going to offer complete protection to an individual's personal data on the Internet. Instead it is proposed that the Government implement a three-pronged approach: implement effective and technology-savvy regulations; develop corporate privacy cultures; and promote public awareness that they as individuals constitute the first line of defence[5]. This approach will ensure that individuals will become "citizens rather than victims of the information age."[6] This report will concentration the data protection legislations in place and outline possible changes, which would hopefully increase the protection currently provided for an individual's personal information on the Internet. The other two recommendations will be considered in brief.

Data Protection Law in Ireland

Currently the provisions of the DPA and regulations made under the 1988 Act regulate data protection law in Ireland. It is a comprehensive piece of legislation, which offers blanket guidelines for all data with an identified or identifiable subject. Personal information is protected at each stage of the flow of data. This is achieved by the establishment of several key principles outlined in S.2 of the Act, i.e., the fairly obtaining and processing principle, the accuracy principle, the purpose principle, the sufficiency principle, the time principle and the security principle. The DPA arose out of our obligations under the Council of Europe Convention for the Protection of Individuals with

[4] Cookie Monsters? Privacy in the Information Society Report by the Australian Senate Select Committee on Information Technologies, November 2000, hereinafter referred to as Cookie Monsters
[5] Ibid
[6] Ibid

regard to the Automatic Processing of Personal Data[7] which is incorporated in Schedule 1 of the DPA. The main aim of the convention was to combat the practice of transmitting data across borders thus circumventing data protection law in one country in favour of a "data haven". The European Union adopted a Directive entitled the Protection of Individuals with Regard to Processing of Personal Data (95/46 EC)[8]. Its aim was to amplify the provisions already set down in the convention and harmonise the law in the European Economic Area (EEA – the EU along with Norway, Iceland and Liechtenstein), thereby promoting the Common Market. This was followed in 1997 by the Council Directive on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (97/66 EC)[9]. The DPA is due to be revised in the near future to implement the terms of the Directive 1995. The first step in this process will be completed on April 1st 2002 when Articles 4,17, 25 and 26 will be incorporated into the DPA.

Analysis of the DPA in relation to the protection of Personal Information on the Internet

When online, a person may perform different functions, eg. Obtain free information, purchase information and good, make friends and contacts and communicate electronically. Based on these different functions, the Internet may be divided into different sections eg. Electronic mail, e-mail, surfing and searching on the World Wide Web (WWW), publications and fora (i.e. newsgroups, chatrooms, directories etc.) and electronic commerce and cyber marketing[10]. The privacy of personal information is challenged in each of these areas.

---

[7] Hereinafter referred to as the Convention
[8] Hereinafter referred to as the Directive 1995
[9] Hereinafter referred to as the Directive 1997
[10] Privacy on the Internet

An Individuals e-mail address may be collected without their knowledge or consent from public areas of the internet such as newsgroups. This is contrary to S.2 .1.a of the DPA which states that "the data or, as the case may be, the information constituting the data shall have been obtained and the data shall be processed, fairly." This provision is wholly unsatisfactory when considered in the light of similar provision contained in the Directive 1995. Personal data may only be collected for "specified, explicit and legitimate purposes." [11] Also, processing must be done "fairly and lawfully"[12] and in accordance with one of the Article 7 criteria, (a) being that "the data subject has unambiguously given his consent." Article 7 is unique to the Directive. Its incorporation into Irish law would be a welcome and necessary change. It's specific language would end the uncertainty surrounding the current legislation.

If an e-mail address is made public, it cannot be used for any other purpose than the one for which it was made, especially not direct marketing[13]. This is a result of the purpose principle in S2(1) (c) (i) and (ii): "the data (i) shall be kept only for one or more specified lawful purposes, (ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes." The Data Commissioner[14] has given an interpretation of the word compatible and S.2 (1)(c)(ii) in Case Study 8 of his Annual Report 1996. He stated that "the strength or weakness of the privacy protection afforded by the Act largely stand or falls on the interpretation of this phrase." Accordingly he adopted a restrictive meaning relying on the U.S. case of Britt v. Naval Investigative Service[15]. It is obvious how beneficial the annual reports are for guidance in finding the corrective interpretation of provisions. It is hoped that a more formal process would be implemented in the future which would make the tasks of both students and lawyers easier when interpreting legislation and advising clients. This would improve the effectiveness of the DPA and

---

[11] Article 6(b) of the Directive 1995
[12] Article 6(a) of the Directive 1995
[13] Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union hereinafter referred to as Recommendation 2/2001
[14] The Data Commissioner is established under s.9 of the DPA. His powers and duties are set down in Schedule 2 of the Act. He is required to be an independent body that must investigate or cause to be investigated suspected breaches of the DPA. He published his findings in an annual report. The current Data Commissioner is Mr. Joe Meade.
[15] United States Court of Appeals for the Third Circuit, 886 F.2d 544

increase the protection it offers to the privacy of personal information in the online environment.

A secondary use which the data may be used for is direct marketing, a tool used by cyber marketing companies to engender business by sending unsolicited e-mails. It is regulated specifically by s. 2(7) of the DPA and S. 14 (b) of the Directive 1995. Section 2(7) provides that if a data subject writes to a data controller[16] and requests him to cease using his personal data for direct marketing purposes, the data controller must, within forty days, erase the data or cease using it for that purpose if it is also used for another purpose. Section 14(b) offers the same protection but its provision are strengthened by the proviso that "Member States shall take the necessary measure to ensure that Data Subjects are aware" of the protections offered in relation to direct marketing[17]. Other countries such as Germany, Austria, Italy, Finland and Denmark have banned the use of unsolicited commercial communications. In Ireland, the question of consenting to direct marketing is unclear. The Commission proposal for a directive on the processing of personal data and the protection of privacy in the electronic communication[18]s sector of July 12th 2000 "favours a harmonised solution based on the 'opt-in' approach,"[19] as set out in Article 13. The opt-in approach protects privacy better than the opt-out options. It is submitted that Irish legislation should either ban the use of unsolicited commercial transactions or adopt the opt-in approach.

In the DPA, personal information is defined as "data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the controller."[20] It is proposed that this is an inadequate definition of personal information. The development of technology on the Internet, specifically, the use of cookies

---

[16] A data controller is defined under S.1(1) of the DPA. It means "a person who, either alone or with others, controls the contents and use of personal data." The restrictions imposed on a data controller are due to be changed by S.I. 626 of 2001, which will implement Article 4 of the Directive 1995

[17] Kosten and Pounder, "The EC Data Protection Directive 1995: An Analysis" (1996) 2 Web JCLI

[18] COM(2000) 385 of 12 July 2000. This proposal is intended to replace the Directive 1995.

[19] Recommendation 2/2002, pg 9, fn 14.

[20] Section 1(1) of the DPA

and web bugs to collect information means the provisions of the DPA can be circumvented and the result in the invisible profiling of individuals. "The cookie is a small file containing an ID number that is place on a user's hard drive by a website."[21] Web bugs are "invisible images that also place cookies on users' computers."[22] A cookie allows a website to track users over a session. In this way a cookie may surreptitiously collect information about the user's browsing habits. The economic importance of this of this information has been recognised by cyber marketing companies. Doubleclick, the largest ad service provider, has agreements with over 11,000 websites and maintains cookies on 100 million users[23]. Cookies collect raw data, which if combined with data, which if combined with data already available to the company may be used to infer new data:

" 1. The country where the Internet user lives.
2. The Internet domain to which he/she belongs.
3. The section of activity of the company employing the Internet users lives
4. The turnover and size of the employing company
5. The function and position of the surfer within this company
6. The Internet Access Provider,
7. The topology of the websites currently visited."[24]

This invisible profiling falls outside the ambit of the DPA because of the inadequate definition of personal data. A more satisfactory definition is that contained in Article 2(a) of the Directive 1995. "Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or *indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identify." (Emphasis added) This is a much broader definition because it covers information, which may directly identify an individual. It is submitted that this would cover information gathered by cookies and web

[21] Privacy and Human Rights 2000 Overview at www.privacyinternational.org
[22] Ibid
[23] Ibid
[24] Privacy on the Internet, pg 16

bugs. As noted by the Cookie Monsters Report, this is an example of "technology-savvy" regulations.[25]

The consent of an individual to process their personal information is a central concept to the Directives. This is illustrated by the Article 7 criteria and Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union. There is an implied recognition of the importance of a valid consent in the S.2 data quality principles contained in the DPA, eg.Data must be obtained and processed fairly[26] and data may only be kept for one or more specified and lawful purposes[27]. By virtue of the Recommendation of 2/2001 a controller must provide certain information to a data subject and place in directly on the screen in order to acquire valid consent. The information to be provided is:

"- the identity of the controller;

- the purpose(s)
- the obligatory or optional nature of the information requested;
- the recipients or the categories of recipients of the collected data;
- the existence of the right to oppose any disclosure of the data to third parties for purposes other than the provision of the requested service and the way to do so (for example, by placing a box to be ticked)
- the information which must be supplied when using automatic collection procedure;
- the level of security during all processing stages including transmission, for example over networks."

These requirements greatly increase the level of protection available to a data subject over the use of personal information. It is proposed that these be implemented into the Irish Act along with the Article 7 criteria.

Regulating the Internet and Improving Public Awareness of the Privacy Risks inherent in the Internet

[25] Cookie Monsters, pg 65
[26] Section 2(1)(a) of the DPA
[27] Section 2(1)(c) of the DPA

Care must be taken when introducing regulations on the Internet not to regulate it to strictly thus rendering the Internet impotent. "Such restrictions may … have the effect of turning one's country into a boreen running alongside the Information Superhighway."[28] Certain characteristics of the Internet make it susceptible to the gathering of information. The TCP/IP protocol is always used as the intermediate layer of protocol on the Internet. A protocol in this context sets down the rules to be observed by two parties in order to exchange information. Three characteristics of the TCP/IP protocol constitute potential invasions of privacy i.e. the route, DNS server and the PING command. The TCP/IP protocol is supplemented by higher-level protocols to provide additional services. The HyperText Transport Protocol (HTTP) is the main type of such protocols. It offers e-mails and discussion for a. The main threats to privacy from this protocol are browsers chattering, hyperlinks and cookies[29].

The EU is considering introducing recommendations, which would require the production of privacy-compliant browsers with the most privacy-friendly default settings. Such recommendations should take notice of the existence of anonymous proxy servers which can hide IP addresses[30]s. Every Internet Service Provider should offer this technology as a free standard feature with an Internet subscription. Individuals should be informed of the privacy risks on the Internet and should be made aware of the Privacy Enhancing Technologies. The Article 29 Working Document recommends that the public sector take the necessary steps to raise awareness of privacy enhancing technologies and support the development of these solutions, in addition to using and promoting them. Another idea being considered by the EU is the labelling of websites, thereby indicating which websites are privacy compliant and best protect the personal information of visitors to the site.

All of these measures would increase the trust that consumers have in e-commerce. At the moment it is at a very low level as is indicated by figures

[28] Kelleher and Murray, Information Technology Law in Ireland (Dublin 1997)
[29] For more information see Privacy on the internet, especially pg 8, 86 & 87
[30] An IP address is a unique identifier of a computer

published in the Irish Times on April 13th 2001. "By 2005 …sixty one percent of Europeans and sixty four percent of Americans will have access to the Net on PC. Yet only 7 per cent of Europeans and 11 per cent of Americans are expected to buy online by then." John MacDonnell in his article 'Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?'[31] believes that a Canadian seal of approval would increase the trust felt by consumers in e-commerce, by "in the long term, a Canadian privacy seal would have to be supplanted by a mark signifying the co-operative efforts of an international group of data protection commissioners, aided by similar input from governments, industry and consumers." If the EU were to implement a privacy seal this would serve to be a guarantee in the minds of individuals of the protection of their privacy on the Internet.

The purpose of the DPA was outlined by the then Minister for Justice, Mr. Collins when introducing the Bill at the Second Stage as being "to provide adequate safeguards to individuals against any abuse of their privacy arising from the automatic processing of personal data concerning them."[32] It is submitted that the DPA falls way short of the mark when striving to provide adequate safeguards for protecting personal data on the Internet. The DPA should be updated to implement the provisions of the EU Directive of 1995[33] and the updated version of the 1997 Directive. Also, privacy protective policies should be fostered among the private sector. Increase debate in the public domain would heighten public awareness. Furthermore regulations for the Internet should be put in place with an aim to protect an individual's personal information. All of these changes would mean an adequate standard of protection of personal information for individuals on the Internet.

---

[31] (2001) 39 Alberta L. Rev 346

[32] 375 Dail Debates, cols 847-8

[33] Cookie Monsters, pg 48; "The Directive 1995 is acknowledged to have established the highest standard for the legislative protection of information privacy in the world."