Journal of Information, Law and Technology

RFID: Radio Frequency Identification OR Real Frailty in Data Protection?

Adrian Bannon
Lecturer in Law
Faculty of Applied Arts
Waterford Institute of Technology
adrian.bannon@gmail.com

This is a Refereed Article published on 24th October 2008

Bannon, A., "RFID: Radio Frequency Identification OR Real Frailty in Data Protection?", JILT 2008(1), <http://go.warwick.ac.uk/jilt/2008_1/bannon>

Abstract

Synonymous with the obvious euphoria and panegyric extolment surrounding the exponential advances in modern science, there is a growing body of weighty privacy concerns uttered over the extent to which the potential ramifications that the commercialisation of certain technological innovations may have. One technology presently inflaming privacy advocates' is radio frequency identification (hereafter RFID), and whether Europe's omnibus data protection regime is up to the mark of adequately protecting individual privacy. Taking some of the more salient aspects of the European legislation, this paper will endeavour to examine whether such concerns are justified, and what if anything, can be done to ameliorate such concerns.

Key Words: Radio Frequency Identification, Privacy, Data Protection.

1. Introduction

Privacy is a quintessential cornerstone of most democratic legal systems (Eschet, 2004).[1] Its importance as a theoretical, social, and philosophical value, have seen it come to be protected and upheld by some of the highest legal standards, constitutions and international human rights treaties. But privacy, like technology and government, is undergoing a vacillating course. The concept of privacy,[2] in our case informational privacy, is relatively new. As noted by one writer (Godkin, 1890 p.12):

> "Privacy is a distinctly modern concept, one of the luxuries of civilisation, which is not only unsought for but unknown in primitive or barbarous societies."

The laws relating to privacy are thus in a full state of evolution and the developments that have allowed privacy to blossom are equally as new.

Concurrent with these rather welcome developments though, is the putative contradiction that privacy is also developing at a time when it can be reduced to very little, and this erosion is progressing quickly due to our continued ingenuity. One of the most recent examples of this ingenuity is radio frequency identification, where the hype attached to the *potential* privacy concerns associated with the technology, it is humbly submitted, seems to wane significantly in comparison to the technology's marketplace momentum. What will be examined in this article will be whether Europe's already under pressure omnibus data protection regime is up to the privacy challenges presented by our continued technological ingenuity.

2. Radio Frequency Identification – A Taxonomy of the Technology

[1] Note, the English words "private" and "privacy" are derived from the Latin *privatus*, meaning "withdrawn from public life, deprived of office, peculiar to oneself.".

[2] The current author does not claim to have any proficiency in proffering a concise conceptualisation of the term 'privacy'. Such an issue has long occupied the minds of far more superior scholars and jurists alike for decades and so is unlikely to be resolved in the current discussion. What the current author will observe is that, while there is undoubtedly a certain intuitive appeal to the thought processes of persons' such as Judge Cooley, Samuel D. Warren and Louis D. Brandeis, Alan Westin and so fourth, none of their definitions have as of yet been accredited as being universally acceptable.

RFID is a simple concept with enormous implications (Finkenzeller, 1999). To paraphrase one writer (Drucker, 1999), it could be to the information revolution what the rail road was to the industrial revolution. The term 'RFID' is a generic expression for technologies that use radio waves to automatically identify individual items. At its core, RFID is an extension of electronic database technology that has been used in the commercial sector for decades (EPIC Workshop Comment, 2004). RFID systems are a subset of a larger class of technology known as automatic identification (Auto-ID) systems. Similar in concept to the Universal Product Code (UPC), RFID devices are the next generation of barcodes. The tags have the ability to scan multiple items simultaneously as well as being able to constantly refer to an item's whereabouts at all times. It is for this reason that RFID tags have famously been termed 'barcodes on steroids' (US Senator Patrick Leahy, 2004). They consist of labels that are placed on merchandise or objects to identify their location. Patented in 1973, the core technology for RFID was initially employed as part of military applications in the 1920s by the British (Stockman, 1948), who through the use of the all 'Identity Friend or Foe' (IFF) system, used RFID signals to confirm the identity of their own aircraft in flight during World War II (Landt, 2005).

No longer an object of wartime nostalgia; the commercial value of RFID, has now firmly sprung the technology from the fusty realms of military history, into those of contemporary political discourse and corporate consciousness. The actual idea of RFID product tracking was developed by Kevin Ashton, a brand manager at Proctor and Gamble (Stein, 2007). In attempting to resolve a growing supply-chain dilemma, Ashton, determined that by placing a small electronic tag[3] on each product, the monitoring and stocking of each cosmetic item could be facilitated. Ashton, somewhat controversially, tested this hypothesis in a store at Broken Arrow, Oklahoma and it proved to be a resounding success (Garfinkel, 2002). Through additional experimentation the technology has grown and improved even more to such an extent that countless new applications have materialised and mainstream distribution now beckons (Cardullo, 2003). It is these additional applications that are prompting concerns from privacy advocates.

3. Privacy and the Law

As of yet there is no specific RFID legislation governing the technology.[4] For this reason the remainder of this article will focus on existing legislation, i.e. data protection, which, in the interim at least and absent any reform in this area, should be largely responsible for the potential governing of the technology. How we treat privacy at a national level however will also be hugely important because while the parameters of data protection law are not strictly confined to electronic data, that is its main focus, and there is a concern that wider ideas of protection could get lost. It is also worth stressing that while the analysis forthcoming will focus primarily on Ireland's implementation of Europe's data protection legislation, it will be suggested that many of the principles/issues expounded will be relevant to the entire legislative model as a whole.

[3] Regarding the tags themselves, there are two main types: active and passive. The main differences between the two tags are there longevity and there power source. Note: there is also what is referred to as "semi-active tags". These are tags that use an embedded battery to power the electronics, but still employ passive response such as radio frequency backscatter for uplink from the tag to the reader. EPCglobal has currently established six classes of tags ranging from Class 0 to Class 5.

[4] There may of course be industry guidelines, codes of practice etc. But as far as the current author is aware (please correct if necessary), there remains in place no RFID specific legislation either within Europe or her Member States. The technology is attracting much more attention and debate in the United States.

3.1 Data protection law is now expected to be the main source of protection where privacy of our electronic data is concerned. In time it may in fact become the only one. This places a considerable burden - both in terms of those seeking to best adhere to the data protection rules - but also on the legislation itself in having a relevant notion of what counts as reasonable with respect to privacy, as well as being prepared for any legal issues that arise due to new technologies such as RFID (Article 29 Working Party, 2005).[5]

What will be concluded in this comment is that data protection - while a pioneering piece of legislation in its own right, propelling the important issue of individual protection of personal data into binding territorial legislation – the existing provisions for reform will need to be further revised, more regularly updated and better reinforced, if it is to have any chance of fulfilling its Herculean goal. Of concern from a Member State perspective could be: the varying degrees of protection afforded to public bodies and private entities under their implementing Act(s); the fact that there have been major changes in technology since the enactment of many such Act(s), changes which could have important consequences; the liberal exceptions enshrined within the implementing legislation; the ambiguous definition(s) of what constitute 'personal data'; and the ever-present issues of resources and enforcement.

3.2 Where RFID generated information (or information generated by any technological means for that matter) is held by public bodies, the scope of the Irish Acts for example seem to be fairly restricted.[6] This does not appear to be the case for private entities. Moreover, while consent is almost always a prerequisite for most data processing in the normal course of events, Ireland's Data Protection Acts appear to be more deferential towards public bodies (O'Dowd, 2005). This is a potential cause for concern since through the widespread deployment of RFID, the State and its subsidiary public bodies, can expect to see an exponential rise in both the amount and type of data it will generate.

The intention here is not to sound crestfallen or downbeat, it is merely to point out that both the Directive and the Acts have their limitations and neither should be seen as being immune from reform (O'Dowd, 2004). In fact, any antipathy that businesses, lawyers, and private citizens could have toward the legislation is potentially attributable to the high expectations they had to begin with. The Directive has governed our privacy for the best part of a decade now[7], yet the question of adequately protecting our privacy remains firmly open.

These concerns, it will be submitted, exist irrespective of any proposed threats from RFID, though RFID as a technology *may* exacerbate them. It will also be contended herein that RFID, while a cause for concern in itself, it highlights the bigger and arguably more important picture that the European legislation is far from watertight and will need to be kept under ongoing reform. That said, and by way of shedding some light on the subject, the

[5] The Article 29 Working Party for example is clearly of the view that some applications of RFID will give rise to privacy concerns.

[6] The central focus of this paper is on the definition of 'personal data' and its processing thereof as opposed to the potentially deferential latitude conferred by the Irish legislation towards public bodies.

[7] Note: Ireland had already in existence data protection legislation (the Data Protection Act 1988) prior to the coming into force of the Directive. The Directive is a continuum of that movement. The Directive was partly implemented in Ireland by the European Communities (Data Protection) Regulations 2001 (SI No. 626 of 2001), and full implementation occurred with the passing of the Data Protection (Amendment) Act 2003. This Act, which came into force on April 10 2003, repealed the 2001 regulations and amended our 1988 legislation so as to bring it into line with the requirements of the Directive. The 1988 and 2003 Acts (hereafter the Irish Data Protection Acts) together constitute the Irish data protection legislation.

European legislation is still in a far better position to deal with any threats from RFID than say, the current legislative schema (or lack thereof) in many other jurisdictions.

4. Introduction to Data Protection

The European Directive on the Protection of Personal Data (hereafter Directive 95/46/EC) sought to harmonise and broaden European data protection law at a higher level of protection than that previously in existence. It represented an ambitious attempt at fully implementing the previously achieved 1981 Council of Europe (COE) consensus on a standard for personal privacy. All EU Member States thus were required to implement the Directive into national legislation by 24 October 1998, and Ireland was no different in this regard[8].

4.1 Overview of the legislation

Firstly, the European approach to data privacy legislation is a pragmatic and proactive one. Within the burgeoning discipline that is Information Technology, it is also a rare example of legislative foresight (Rowland and MacDonald, 2005). The legislation is however at times technical and complex (Hedley, 2006, p.79-102). This is perhaps partially due to the divergent interests at stake, but it may also be because the main motive driving the whole debate is arguably the free flow of information and not privacy (Hedley, 2006).[9] This is evidently reflected by the term 'data protection', which is in itself somewhat of a misnomer. Data Protection does not seek to protect data *per se*; rather it seeks to protect the individual from unwanted or abusive uses of their personal data. Nor for that matter does it protect against abuses of RFID; the Directive is a form of baseline technology-neutral legislation. While this generality avoids many of the pitfalls of say, a technology-specific model (Hildner, 2006) such as that adopted in the US,[10] the vacuous remit of the European legislation does mean that while all technologies are likely to be protected against, there *may* be discrepancies in the degrees of that protection.[11]

4.2 As a result of its generality data protection legislation within the EU, it would seem, has been split into various schools of thought. For present purposes we will limit ourselves to two of those, though of course there are many more. On the one hand, there are those that see data protection as marking the high level water mark of privacy protection. On the other, there are those that see data protection as nothing more than a needless bureaucratic process. A protagonist of the latter school, British Conservative Party politician John Redwood for example, has recently called for the data protection regime to be scrapped altogether (Redwood, 2008). The wisdom of such a move is questionable. Apart from the semantic

[8] Ireland had already in existence the *Data Protection Act 1988* (No.25 of 1988). But in response to increasing pressure the European Commission, Ireland introduced the *Data Protection (Amendment) Act 2003* (No 6 of 2003) by Order (SI No. 207 of 2003) which sought to fully transpose the Data Protection Directive into Irish law. This new Act repealed the European Communities (Data Protection) Regulations 2001.

[9] Although frequently now discussed in terms of the rhetoric of rights, the original objectives of data protection rules were arguably much less aspirational.

[10] By specifically legislating for one technology over another, Congress runs the risk of making one technology potentially disfavourable relative to another emerging technology, whose intrusions on consumer privacy could be equally as potent. One could for example, circumvent RFID-Specific legislation by using an alternative technology with similar capabilities but that is not legislated for. There is of course also the issue of inconsistency since in the absence of Federal-made law; several US States' could implement legislation differently, if at all. This has already happened in the case of RFID.

[11] This is of course speculative on the author's point as there is little by way of current empirical evidence to substantiate claims that one set of technology is significantly better protected than that of another.

significance of the Directive,[12] scrapping the data protection regime would likely undo the long and arduous years it took to reach a territorial consensus on the legislation to begin with. More significantly though, and where Redwood has not been as expedient, is in the offering of a viable alternative. The problem with scrapping the existing regime is that creating an alternative that is more comprehensive or works better than data protection is a difficult undertaking. Not only would any new regime have to prove more rational, it would also have to prove more acceptable to a now wider variety of people in very different national settings.

The current author, while firmly against the endorsement of a proposal as radical as Redwood's, is nevertheless sympathetic to many of the reasons which may have prompted such a view. For instance, the broad notion of the Directive combined with its failure to adequately define certain key terms has led to various interpretational difficulties. Where definitions have been provided, they have been couched in such broad terms that any attempts at conceptualisation proves difficult. A classic example is the definition of 'personal data'. Personal data is at the core of data protection law and yet it remains one of the most amorphous aspects of the legislation.

4.3 Personal Data

Article 2a of the Data Protection Directive defines 'personal data' in the following terms:

> '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 identity' (Art. 2(a) of directive 95/46/EC).

The Directive further provides that the above definition applies only to the processing of personal data where the processing is wholly or partly by automatic means, or where it is non-automated processing data which forms part of a filing system or is intended to from part of a filing system (Art.3 of Directive 95/46/EC). The Directive therefore considers: (i) whether the information relates to an identifiable individual and, (ii) the two different types of processing (automatic and non-automatic) within a filing system, which bring information within the scope of the Directive. Before going on to processing however, it is necessary to look at the definition of 'personal data' first.

The definition in Article 2 is fairly broad in that the individual need not be directly identifiable from the data concerned. At face value therefore, where the data is enough in itself to identify a particular individual, such as one's name or their picture, it unequivocally appears to come under the remit of 'personal data'. Potentially less certain (though there is an ever-growing body of opinion suggesting otherwise), is the scope of the definition to less direct and numerical identifiers. Will alphanumeric RFID serial numbers for example, fall within the remit of the definition[13], or will they suffer the previous ambiguities associated

[12] The Directive is binding on all EU Member States with agreements in place for countries of the European Economic Area (EEA). In managing to reach a wide level of consensus across the Member States on a growing issue; the Directive is not only a fine example of cross-border cooperation and legislative foresight, but it also sets Europe apart as being at the forefront of protecting its citizens' informational privacy.

[13] Use of one's mobile phone or Tesco loyalty card for example is not always limited to the use of the actual owner. Cards can be shared and phones can be borrowed. In these situations the personal data required is not that of the actual data subject but that of another.

with identifiable data such as telephone numbers and postal addresses? Take the example of email addresses. Frustrating in any attempts at regulating Internet SPAM has been the legal question of whether email addresses constitute personal data because if the address is all the spammer has, does this constitute personal data? The matter is complicated by the fact that there are for example, already hundreds and in many cases thousands of e-mail addresses all denoting the same name, or permutations of very similar names.[14]

4.3.1 The issue is an important one because most data does not clearly identify its subject, but is within the legislation if its subject can be identified from that data and from other information which is, or is likely to come into, the possession of the data controller. But determining whether a 'natural person'[15] can in fact be identified from data which is linked to that person and that which identifies him is something of a moot point.[16] The two are not the same. Even if we revert to a more traditional and definitive means of identifying someone, such as one's name, we can see that the issue is not clean cut. The author's own name for instance, 'Adrian Bannon' will not always be personal data because there are other individuals with this name (ICO Guidelines 2007 p.6).[17] Only if the name was combined with other uniquely personal information such as my address, identification number, place of work/study, or telephone number could it sufficiently identify one Adrian Bannon from another.

Furthermore, information that is not personal data today can become personal data down the line. For example, you may not know the name of the red haired middle-aged blind man, with a golden retriever guide dog and who regularly walks the grounds of Edinburgh University, but you are still able to identify him. Not knowing someone's name or personal data therefore, does not mean you cannot identify a particular individual. That said though, the confusion between personal data and identity is one that continues to persist. Efforts at qualifying the meaning of 'identifiable' stem from a long-running contretemps in COE circles as to the effort required to render non-nominate data as 'personal data'.

4.3.2 Outside the scope of the definition is data that has been anonymised. But what constitutes 'anonymised' or what exactly is required under this provision? Will for example alphanumeric data derived from an RFID serial tagged object constitute anonymised data or will it be classed as 'personal data'? Like the issue of direct and indirect identifiability above, a lot of work has been carried out in this area and this is to be welcomed, especially with new and more complex technologies' coming on stream. Taking this into consideration, the simple answer is it will depend. It will depend on the strength of the link to the identifiable individual concerned. This is potentially troublesome however, since the simple act of purchasing an RFID tagged product in one superstore may not constitute personal data today, but may do so in the future. RFID tags are promiscuous by nature – that is they possess the

[14] The world's most common name for example, 'Mohammed' could be mohammed1@hotmail.com, mohammed2@hotmail.com, mohammed99@gmail.com and so on. Note also the email exemption provided for under Article 13 of the Electronic Privacy Communications Directive (Directive 2002/58/EC, [2002] OJ L 201/37).

[15] Note the phrase 'natural person' is to denote that the person must be a living human being. Deceased people or artificial persons such as governments or companies would not be protected, though the employers of such entities obviously would be.

[16] Some Member States such as Austria, Denmark, Italy and Luxembourg protect the personal data of 'natural' and 'legal persons'. Others such as Ireland and the United Kingdom only protect the personal data of 'natural' persons.

[17] There could be an Adrian Bannon father and Adrian Bannon son for example, and both could work in the same place of employment.

ability to communicate with multiple readers. RFID tags are also persistent identifiers that can collate and aggregate data through time. Put alternatively, data associated with a tag number is theoretically unlimited and can be constantly augmented as new information is collected. Therefore, what may seem as anonymised anonymous data to us may in fact turn out to be distinctive data to someone else.

4.3.3 This raises another pertinent issue. At such a low price, tags and portable readers are economically feasible for surreptitious third parties. Thus, while the data on the tag might amount to no more than an EPC Serial Number, an interested and determined party with access to the appropriate database, for example, one that records credit card purchases, could link a purchased item to an individual's name and profile. This is because RFID, whilst not a *de facto* indicator of one's identity; it will render people becoming more identifiable through their possessions. This identifiability is only going to improve as the tags become more advanced in their reading capabilities. In this regard, data controllers such as Tesco, Wal-Mart and so forth, who contend that the data they hold does not allow the identification of individuals, should be expected to review their policies regularly in light of new technologies such as RFID. Such concerns have long been reflected by the British Information Commissioner's Office (ICO) who notes that:

> "When considering identifiably it should be assumed that you are not looking just at the means reasonably likely to be used by the ordinary man in the street, but also the means that are likely to be used by the determined person with a particular reason to want to identify individuals. Examples would include investigative journalists, estranged partners, stalkers, or industrial spies." (ICO Guidelines 2007 p.1)

4.3.4 Information therefore, can count as personal data in one person's hands but not in another's. The data extrapolated from an RFID reader and at the knowledge of the consumer in Tesco for example, to collect data about individuals in a supermarket, may not constitute personal data about the individual *per se* as it is not being processed to learn anything about a particular individual. Tesco may just want to know how much of each product it sells and at what times. Furthermore, it may just use the crowd data to analyse general customer movements within the store. By establishing the areas of the store and aisles consumers frequent most, Tesco can use these areas to distribute goods they may wish to shift more quickly or goods which attract the biggest profits. In these circumstances Tesco is not learning anything about its individual customers, rather, it is trying to find out crowd movements and crowd purchases as a whole.[18] The estranged partner, stalker, terrorist, identity thief or private investigator with their own private reader on the other hand, may use the data acquired for building up some kind of a profile of that individual and their personal details (ICO Guidelines 2007, p.2).[19]

4.4 *Durant*

One case that has significantly altered the concept of personal data is the British decision in *Michael Durant v. the Financial Services Authority*.[20] The case involved a dispute between Michael Durant and Barclays Bank. As is an individual's right under the data protection

[18] This is not to say Tesco will not use such data for more refined purposes – something we will see when we discuss personal data under the data quality principles.
[19] The ICO uses the example of a crowd photo taken by a journalist to show people having a good time at a rock concert and a similar photo taken by a police officer for law enforcement purposes.
[20] *Durant v FSA* [2004] FSR 28.

legislation, Durant made a subject access request under the British Data Protection Act 1998 (section 7). The reason for Durant's request was to obtain 'personal data' about him which was held by the Financial Services Authority (FSA). The FSA, in refusing to provide all the information requested by Durant, argued that not all of the data constituted 'personal data' as defined by the legislation. Furthermore, even if it did constitute 'personal data' for the purposes of the legislation, it was not contained within a 'relevant filing system'.[21] The principal argument by Durant was that both the definitions of 'personal data' in the Directive and the DPA suggested a 'wide and inclusive definition of "personal data" and one which 'covered any information retrieved as a result of a search under his name, anything on file which had its name on it or from which he could be identified or from which it was possible, to discern a connection with him.' Significantly the court, in the form of Auld LJ, disagreed. They came to the conclusion that the definition was much narrower than that.

4.4.1 While Durant is but one case in only one jurisdiction, its short term significance should not be dismissed. It confirms that in the UK at least and for the time-being, parts of documents can count as personal data without the whole document counting as such. By ruling that - just because a document contains the complainant's name, it is not necessarily personal data - the English Court of Appeal has changed the perception of how wide a definition of personal data could be. What this *could* mean for a technology like RFID is interesting, since not all RFID applications will offend the individual's privacy or family life, and not all RFID data will be biographical in a significant sense. Will for instance, the simple act of buying a tin of beans, a litre of milk or a loaf of bread be 'biographical in a significant sense'?

More importantly though, and deviating away from this solitary interpretation, the case serves as a potentially illustrative example of the increasing hostility various Member State Governments' now have for data protection legislation and its significance. By disregarding the threat in Durant, the British Judiciary has effectively undermined a significant feature of the legislation. This *de minimis* definition of personal data by the English Court, it is humbly submitted, sets a potentially dangerous precedent for future data subjects seeking to exercise their right of access. Crucially, the decision in *Durant* has already been applied and approved in *Johnson v Medical Defence Union.*[22] Little wonder then, *Durant,* which has already attracted adverse comment is now under European review and has led to the Office of the British Information Commissioner to draft new guidelines (ICO 2007).[23]

4.5 Personal Data in Ireland

The above cases of *Durant* and *Johnson*, while important for the reasons cited above; they are English decisions and so are of no automatic legal force in Ireland, Italy, Germany or elsewhere. Nor for that matter do they set any automatic guide of how other courts, if faced with the issue, would define personal data. From an Irish perspective thus, and in the absence of any immediate case law on the matter, it is necessary to look at the legislation itself.

Personal data under the Irish DPA is defined as:

[21] As we discussed above, the definition of personal data applies only to the processing of personal data where the processing is wholly or partly by automatic means, or where it is non-automated processing data which forms part of a filing system or is intended to form part of a filing system.
[22] *Johnson v Medical Defence Union* [2004] EWHC 347.
[23] These very recent guidelines refer only to 'personal data'. The issue of 'relevant filing system' will be the subject of review in the near future.

> 'data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the data controller' (section 1(1) of the Irish DPA).

Like that of the Directive, this is a broad definition and the individual need not be directly identifiable from the data concerned. As expressed in the definition, the legislation applies as long as the data subject can be identified from the data in conjunction with other information. Significantly, such information need not be in the possession of the data controller; all that is required under the Act is that is that the information is *likely* to come into the possession of the data controller. By way of an example, if an employee is identified in a database by an employee number or RFID badge and the employer has or is likely to get possession of the key which links the number to the individual concerned, the data held by the employee about the individual, it would seem will be covered by the Act (MacDonagh and Crowley, 2005, p.209).

4.6 Processing of Personal Data

Processing of personal data forms the main part of data protection and for this reason is hard to succinctly surmise in any comprehensive manner. Broadly speaking however, the processing of personal data is not banned. It is allowed provided the processing meets specified, explicit and legitimate purposes. Like the broad definition of 'personal data' provided for in the Directive, the term 'processing' is couched in similarly generous terms:

> 'processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction …' (Art.2 of Directive 95/46/EC).

The broadness of the term 'processing' suggests that it includes just about any activity involving the data. For instance, it seems to include just about anything from: obtaining, organising, storing, altering and destroying. Apart from the protection afforded to personal data by the data quality principles,[24] the Directive imposes additional obligations on data controllers in relation to the processing of personal data, particularly 'sensitive personal data'. The processing of data under the Directive is outlined in Articles seven and eight. The former of these Articles governs the processing of non-sensitive data, whereas the latter governs the processing of sensitive data.

4.6.1 *'Sensitive personal data'*

Of interest under the whole issue of 'personal data', is its subcategory, 'sensitive personal data'. Processing of data under this category is qualified under the Directive (Art.8 [Para's 2-7] of Directive 95/46/EC). Sensitive data is defined in Article 8(1) of the Directive as 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. Definitions of sensitive data have tended to vary between the Member States, with some defining sensitive data more widely than others. The Irish DPA for example, includes all of these but curiously

[24] The Data Principles are discussed below.

broadens the list in the Directive to include the following three: (i) 'philosophical opinions'; (ii) personal data as to the commission or alleged commission of any offence by the data subject; and (iii) personal data as to any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings (section 2, Irish Data Protection (Amendment) Act 2003).

Given that stricter controls apply to this category of personal data; the list as pointed out by Hedley (2006, p.85), is a particularly curious one, since the criteria it sets out (racial origin, gender, political beliefs and so on) denote much that is in practice not actually private. Also of importance here is that any personal data can be or become sensitive depending on its context. For example, a subscription list is not on the list of sensitive data, if it is for a certain type of religious or ethnic magazine or newspaper; it suggests membership of or interest in a specific religious or ethnic group. More clarification will also be required, especially if as expected, biometric forms of identification become more common.

4.6.2 *Consent*

Article seven, as we have discussed, lists an array of circumstances in which the processing of personal data is permissible. Article eight prohibits the processing of personal data, but goes on to list six circumstances in which the prohibition does not apply.[25] The first of these conditions, 'unambiguous consent' by the data subject, is an interesting one. Taking the provisions of these two Articles together, it would seem that unless the specific exceptions apply, the processing of both sensitive and non-sensitive data can only be legitimised by the consent of the data subject. But such consent is qualified by the adjective 'unambiguous' with respect to non-sensitive data and by the adjective 'explicit' with respect to sensitive data. Seeing as consent is the very nexus of privacy law, it seems odd that there are varying degrees of qualification placed on such a fundamental issue in the two consecutive Articles. If consent is to be construed as unambiguous (and ideally it should where privacy legislation is at issue), then there should be no room for doubt as to its exact meaning.

Yet this is exactly what has happened. The type of consent referred to in Article 8 (explicit); suggests a higher standard of proof than that of Article 7 (unambiguous), in which the consent is distinctly stated and cannot be implied. Interestingly, the explicit consent for the processing of non-sensitive personal data had been initially proposed when the Irish Data Protection (Amendment) Act was at its Bill stage (MacDonagh and Crowley 2005, p.229). But this threshold was subsequently dropped at the committee stage and there now remains no definition of consent in the Act. All that is required under current Irish law is 'consent' and this consent operates free from any qualifying adjective. Reverting back to the Directive, Rowland proffers the view that, the qualification 'unambiguous' seems to strengthen the argument that the consent must entail a clear indication of the agreement of the individual, whereas the use of the qualification 'explicit' suggests that the fact that the consent has been given must be established beyond doubt (Rowland and MacDonald 2005 p.327). Whatever the reason, divergent interpretations and qualifications for something as important as consent, could prove problematic where RFID or other processing technologies of that matter come into the equation.

[25] Where for instance: the data subject has unambiguously given his consent; or where processing is necessary for the performance of a contract to which the data subject is party; processing is necessary to protect the vital interests of the data subject; processing is necessary for the legitimate interests pursued by the data controller and so on. Article 8(2) of Directive 95/46/EC.

4.7 Processing and the Irish DPA

The 1988 DPA defined processing as performing automatically logical or arithmetical operations on data (section 1(1) 1988 DPA). Processing under the 2003 DPA is more closely aligned to the definition in the Directive and includes any action that can be undertaken with data, namely:

(a) obtaining, recording or keeping the information, or data,
(b) collecting, organising, storing, altering or adapting the information or data,
(c) retrieving, consulting or using the information or data,
(d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or
(e) aligning, combining, blocking, erasing or destroying the information or data.

The situations in which processing is permitted to occur is set out in sections 2A and 2B. The first of these, section 2A, specifies that personal data should not be processed unless the data protection principles in section 2 and the conditions specified in 2A are complied with (Macdonagh and Crowley, 2005). The principle condition of section 2A is that consent be given, although the requirements of 2A can be satisfied by a range of other ways, for example, where the processing is necessary for the performance of a contract.

In addition to the processing exemptions listed under Article 8 of the Directive, Member States are permitted for reasons of 'substantial public interest' to lay down further exemptions. Guidance as to what constitutes 'substantial public interest' was set out in some of the recitals of the Directive (Recitals 34-36 of Directive 95/46/EC). These would include scientific research, government statistics and compilations of political opinions in the operation of the democratic system. Frustrating from an Irish perspective, section 2B of the Irish DPA 2003 includes a ridiculously long list of factors it regards as being of 'substantial public interest'. Important issues as to their inclusion remain unanswered. In the absence of any case law on the nature of these exemptions, additional attention to the wording of the Directive and COE 108 for a more detailed construction will be needed.

4.8 Data Quality Principles and the DPA

Instead of using the term "data quality", Irish Law has chosen to specify the obligations of a data controller. There are seven such obligations under the Irish legislation (section 2 2003 DPA). While the semantic significance of these principles should not be dismissed, there practical application is questionable. In the discussion that follows we will demonstrate their impracticality to RFID. It should be noted however, that these concerns exist in general and have not been instigated by the arrival of RFID.

(i) *Fair obtaining and processing of personal information*

Prior to the 2003 DPA coming in to force the meaning of "fairly obtaining and processing" was unclear. The Irish 1988 Act made little if no attempt to explain the concept. The 2003 Amendment Act in implementing Article 10 of the Directive has remedied this defect to the effect that information that is collected directly from the data subject cannot be regarded as being fairly processed unless the subject is aware of the following:

(a) the identity of the data controller, or if as frequently the case with public bodies their nominated representative,

(b) the purpose for which the information is collected and,
(c) the purpose or purposes for which the data are intended to be processed and,
(d) other information which is necessary having regard to the circumstances to enable the processing of the data to be fair to the data subject including:
    - the recipients or categories of recipients of the data,
    - whether replies to questions asked for the purpose of collection of data are obligatory and the possible consequences of failure to reply,
    - the existence of a right of access to the data and the right to rectify the data.

Remediation of this definitional deficit while important (Bainbridge, 2005) it does not mean that all information generated from RFID will be obtained and processed fairly. For instance, two important exceptions to the requirements of fair processing have been set out in section 2. These include section 2(5)(b) and section 2(3). The latter of these exceptions has to do with law enforcement and the all encompassing 'national security'. The former exception provides that use for a purpose which was not disclosed at the time the data was obtained does not, of itself, mean this principle has been breached. Taking the example of the average consumer shopping in Tesco; this provision would seem to imply that while we must be notified that the initial purpose of collection will be to monitor stocks and generate consumer discounts, Tesco would not be precluded from using the data to see how long we spend in particular aisles, where we spend most of our time and so on. Even where it did inform us of additional purposes, it could do so in a non-obvious manner such as the utilisation of small print or signage situated only in aisles that are less frequented. This is worrying. On the one hand, our privacy is not being appropriately safeguarded because the obtaining is allowed to take place to begin with, and on the other, we may not know the full purpose of any subsequent processing. It is this subsequent processing that could be most detrimental in the context of RFID.

(ii) *Data is accurate and complete and where necessary up to date*

Section 2(1) (b) requires that data should be accurate and complete and, where necessary kept up to date. This provision replicates that of the Directive (Art.6(1) 95/46/EC). What constitutes 'accurate' is not entirely clear. Some guidance has been provided for. It stipulates that data will be considered to be inaccurate if it is incorrect or misleading as to any matter of fact (section 2(1)(b) of the 2003 Act). It would appear therefore that protection does not extend to data constituting an opinion. But distinguishing fact from opinion is no easy task – a fact reflected by recent case studies on the matter (Irish Data Protection Commission Office).

In addition, ensuring the accuracy of the data and revealing its source is only required if and when an information request is received thus giving ample time for the controller to rectify any wrongs. This is off-putting to the data subject for two reasons: (i) so few consumers are aware or even care about what data is held on them; and (ii) the absence of a remedy for data that is inaccurate but that the controller took reasonable care to ensure was accurate. Moreover, the requirement to keep data up to date is not absolute because it only applies where 'necessary'. What will constitute 'necessary' from the oceans of data generated from RFID is anybody's guess. On a final point, it should be noted that this requirement is concerned less with the protection of a privacy right than it is with imposing a technical requirement on data controllers to design and maintain their databases properly.

(iii) *Data shall be obtained for only one or more specified, explicit and legitimate purposes*

The purpose of this principle is to limit the scope for data controllers to collect information for broad and ill defined purposes, in particular, purposes which have not been thought of at the date of collection. This principle is clearly important in the context of RFID where the one technology can fulfil a multitude of purposes. In theory, the objective of this provision is admirable. It provides legal recognition that as a technology RFID is especially invasive because it threatens to make it extremely easy for companies to gather, archive and utilise private data for numerous purposes.

How effectual this provision is in practice is dubious. It would, after all, be criminal in capitalistic terms for companies like Tesco not to profit from the valuable information they accumulate about us when we shop. Worryingly though, data protection does not prevent the sharing of data, it only protects abuse of that data. The seemingly frivolous caveat, that the sharing is to be notified to the consumer, seems unworkable here. This is reflected in this jurisdiction where, already, the greatest number of case studies to the Data Protection Commissioner has arisen under the purpose specification principle. But this is only the tip of the iceberg - the bulk of consumers as we know, rarely appreciate the summative value of their personal information - nor how technologies (such as RFID) can collect, process and generate data. In this regard, they are ill prepared to protect their privacy let alone be in a position to bargain with it.

(iv) *Data shall not be processed in a manner incompatible with that purpose*

The main reason for this principle is to prevent information that is held by data controllers from being reused and sold. Operation of this data quality principle is well illustrated by analysing some of the Data Protection Commissioner's case studies. One case (case study 2/2000) concerned a secondary school teachers' strike in 2000. The Irish Department of Education sought to restrict payment to members of a particular trade union, and sought to do this by using union membership data it had held for the purpose of collecting union dues. For its part, the Department argued that the terms of its registration with the DPC allowed them to use the data as they had done. The Commissioner however, disagreed, and held that the Department could not legitimately rely on the broad purpose description that it had used when registering as a data controller to displace the actual purpose for which the data was collected. Seeking to use the data for restricting payment was an entirely new purpose that was unthought-of when the data was being obtained.

(v) *Data shall be adequate, relevant and not excessive in relation to the stated purpose or purposes for which it was collected*

Section 2(1)(c)(iii) of the Act states that the data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed. The wording here mirrors that of the Directive (Art.6 (1)(c) 95/46/EC). Like the other principles, this principle is difficult to enforce and it will be difficult to objectively review in many cases. Some situations may prove straightforward, others however may not. RFID by its very nature is designed to collect an excessive amount of information through space and time. When viewed separately a lot of this data will be irrelevant. But RFID tags are persistent identifiers through time and so the real value of the data generated from the tags will be predicated upon the length of time it has to operate. For instance it might not be relevant that Mr. X bought a bottle of whiskey at the weekend but it starts to become relevant information when it shows Mr. X buying a bottle of whiskey every week. In a case study on the issue of the relevancy of certain questions on a motor insurance company's application

form, the Commissioner found that details of a person's marital status as being irrelevant to the question of motor insurance. He added that questions of this nature should be deleted (case study 1/2002).

(vi) *Data shall not be kept for longer than necessary for the purpose or purposes for which it was collected*

Section 2(1)(c)(iv) of the Act provides that personal data shall not be kept for longer than is necessary. Like the principle above, the requirement that data should not be kept for longer than necessary is obscure. This is especially true of the public sector where certain information will often be retained for the lifetime, and beyond, of individuals. Some useful guidance as to time has been provided by the DPC. In a complaint relating to the keeping of minor convictions on file by the Gardaí for an unlimited period of time, the DPC held that this principle had not been infringed since Ireland had no provisions on "spent" convictions (case study 13/1996 p.25). The Commissioner did however state *obiter* that the keeping of information indefinitely did not accord with the spirit of the Act. This is unlikely to upset data controllers too much, since saying something does not accord with the spirit of the Act, does not mean it is in contravention of it.

(vii) *Appropriate security measures shall be provided for*

By itself this provision is not particularly effective in encouraging data controllers to be more vigilant with personal data. Prompt action by the data controller can absolve them of any recriminations. Moreover, the reality as we have seen above is that many breaches of security are rarely, if ever, brought to the attention of either data subjects or the DPC. This is a fundamental flaw of the legislation and typifies the problem of enforcement in general.

4.9 Enforcement

Data protection legislation with its provision for data protection commissioners in each signatory State is actually a more purposeful way of safeguarding individual privacy by governmental agencies and the like, than say a US system of self-regulation and market forces. But this only applies if the EU legislation is properly enforced - something the current author remains fervently apprehensive about. Compliance with the data protection in this jurisdiction falls under the remit of the Data Protection Commissioner (DPC). The powers of the Irish DPC are set out in the 1988 and 2003 Acts. Powers conferred include: the right to investigate and prosecute complaints; the power to search and seize documents; the power to issue enforcement notices, and the allocation of fines. Fines vary from Member State to Member State with the current threshold of fines in this jurisdiction ranging from €3,000 and €100,000.[26] Significantly there is no provision in the Irish legislation for imprisonment of data controllers. This is a major weakness in the enforcement of the legislation but it is not the only one.

For instance, if a defendant thinks that the DPC is acting *ultra vires*, then the matter can be referred to the Irish Circuit Court (Section 26, Irish DPA 1988). But the whole enforcement regime is premised on the somewhat spurious requirement that, the onus lays with the data controllers to identify themselves, the data they possess, and to whom they disclose the data too. Is this a comforting state of affairs where private third parties and unscrupulous retailers

[26] In the UK for example fines range from £5,000 to an unlimited amount.

widely deploy RFID tags? One would suspect not. Of even greater concern is the rate of implementation in Ireland, where the roll out of protection is extending to only certain controllers and only certain types of data. This non-uniform approach creates an uneven playing field and potentially facilitates circumvention of the legislation by certain controllers. Also of concern where the issue of enforcement is at play, is the onus on private individuals to report suspected breaches of their private records. The covert and passive nature of RFID, coupled with individuals' general innate lethargy to complain and investigate proposed privacy violations, is troublesome. It is, after all, already well documented that the vast majority of consumers will trade their privacy, either cognitively or otherwise for the sake of in-store loyalty points or discounts or where they are unsure as to how their personal data will be put to use.[27]

5. Conclusion

Developing legislation for an area as complex as privacy is a governmental nightmare. As the analysis heretofore has attempted to demonstrate, the brisk technological vicissitudes in the area alone ensures most governments place the issue on the long finger until it can be ignored no longer or until they get the coercive kick from Europe. Fortunately, European States' like Ireland, Scotland, and Britain have got this coercive kick, but it may not be enough. This is because, personal data is typically at its most vulnerable when it is being transmitted across networks and the more people that have access to data, the more likely they are to abuse it. The current article has examined RFID, and has endeavoured to explain that if RFID achieves widespread roll out, then the amount of data being transmitted across networks will sore exponentially. The effects of this from a social, economic, cultural and legal realm are important.

Present analysis has focused on the legal realm and how RFID tags have potentially a great significance for data protection law, since they are arguably a very good example of where data protection legislation should work but may not.

Motivation for this omnibus legislation and its ambitious development was initially centred on the whole notion of fear and technological ingenuity. The real fear now however seems to be over our legislative ingenuity and its inability to fulfil its intended purpose. This is regrettable and concerning. The coming into force of Directive 95/46 EC and her other legislative accompaniments were supposed to assure Europe's citizens that their privacy would be protected when they adopted new forms of information technology. And yet the Article 29 Working Party Group in its position paper (2005, p.8) has noted that: "… not all data collection by RFID technology will fall within the scope of the data protection Directive …"; but, "… there will be many scenarios where personal information is collected through RFID technology, the processing of which is covered by the data protection Directive." Such concerns seem reflective of the Redwood school of thought above; namely, we are still unclear as to what data protection covers or should cover, but wholly aware of what it can cost. Given the impending widespread deployment of item-level RFID tags, it is suggestibly submitted that legal boundaries and more particularly the exact scope of personal data, should be established quickly.

[27] In the case of *Bodil Lindqvist* for example a Swedish church maintenance worker and volunteer was fined for creating a webpage detailing information about herself, her husband and eighteen other church volunteers without their permission. *Bodil Lindqvist* [2004] 1 CMLR 20, [2004] QB 1014

By way of final thought, it is critical to stress that privacy concerns are not unique to RFID. RFID is but one of a long list of new technologies eliciting some form of privacy concerns and so a degree of perspective is needed. RFID is also only in the nascent stages of its development and so its full effects, and predictions of those effects, are not yet known. Even not knowing its full effects, many will still posit the view, and perhaps legitimately so, that because the vast majority of societal change and technological development only ever occurs gradually and incrementally; no singular change and no single technology will ever tilt us over the precipice of our privacy protection. To constantly adopt this approach however is to also deny the somewhat orthodox equation that, through time; incremental and gradual frequently translate into substantial.

Accordingly, while many techno-privacy concerns, it is crucially submitted, can be grossly over exaggerated, many others are not and informed concerns need to be taken seriously. So while RFID could in theory turn out to be no more troublesome than its predecessor, the UPC, it is still representative of the trend associated with practically all powerful modern technologies; namely (i) its development is not occurring in a technological vacuum, and (ii) it is being pre-designed to converge with additional technologies. The nub of all this therefore, is that it is crucial to understand, publicly debate and be circumspect of *all* powerful technologies, not just up-and-coming technologies such as RFID. This is because unless each new technology and each new development are carefully scrutinised and understood as one fragment of the larger surveillance mosaic that is being rapidly constructed around us; we will not be suitably aware of the incremental loss of our privacy or the perfidious hype of detrimentally overstating the actual capabilities of a particular technology or set of technologies.

References:

Books

Bainbridge, D (2005), Data Protection (2nd Ed.) (St Albans: England).

Finkenzeller, K (1999), RFID Handbook: radio-frequency identification fundamentals and applications; (Trans. Rachel Waddington) (Chicester: John Wiley).

Hedley, S (2006), The Law of Electronic Commerce and the Internet in the UK and Ireland (London: Cavendish Publishing)

McDonagh , M and Crowley, L (2005), Ireland: International Encyclopaedia of Laws – Cyberlaw (The Hague: Kluwer International)

Rowland, D and MacDonald, E (2005), Information Technology Law (3rd edition) (Cavendish: London).

Journal Articles

Article 29 Data protection Working Party (2005), 'Working Document on data protection issues related to RFID technology' Document 10107/05/EN, 19 January 2005 [available online] at: <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf>.

Cardullo, M (2003), 'Genesis of the Versatile RFID Tag', (16 June, 2003) RFID Journal, [available online] at: <http://www.rfidjournal.com/articleview/392/1/2/>.

Data Protection Commission, 'Annual Case Study Reports', [available online] at: <http://www.dataprivacy.ie>.
Drucker, P F (1999), 'Beyond the Information Revolution', Atlantic Monthly, 284(4), 47-57

Electronic Privacy Information Center (2004), RFID Workshop Comment to the Federal Trade Commission (FTC) – 'Radio Frequency Identification: Applications and Implications for Consumers', June 21 (2004) [available online] at: <http://www.epic.org/privacy/rfid/ftc-comts-070904.html>.

Eschet, G (2004), 'A New challenge to Privacy Management: Adapting Fair Information Practices to Radio Frequency Identification Technology', (2004) [available online] at: <http://papers.ssrn.com>.

Garfinkel, S, 'Adopting Fair Information Practices to Low Cost RFID Systems', [available online] at: <http://www.simson.net/clips/academic/2002_ubicomp_RFID.pdf>.

Godkin, E L (1990), 'The Rights to Privacy', The Nation, 25 December 1990.

Hildner, L (2006), 'Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level', Harvard Civil Rights-Civil Liberties Law Review, 41, 133

Information Commissioner's Office (2007), 'Data protection technical Guidance: Determining what is Personal Data', [guidelines available online] at: <http://www.ico.gov.uk>.

Landt, J, 'Shrouds of Time – The history of RFID', [available online] at: <http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf>.

Leahy, P, 'The Dawn of Micro Monitoring: Its Promise and Its Challenges to Privacy and Security', [available online] at: <http://leahy.senate.gov/press/200403/032304.html>.

O'Dowd, M (2004), 'Data Protection – An Overview', Cork Online Law Review, 3, [available online] at: <http://colr.ucc.ie>.

O'Dowd, M (2005), 'The Privacy Implications of a National Identity Scheme', LL.M Thesis (Pouladuff: University College Cork).

OUT-LAW.COM (2007), 'Information Commissioner updates personal data guidance', The Register, (31 August, 2007) [available online] at: <http://www.theregister.co.uk/2007/08/31/ico_personal_data_guidance/>.

Redwood, J, Online Blog [available online] at: <http://www.johnredwoodsdiary.com/?p=261>.

Stein, S G (2007), 'Where will Consumers find Privacy Protection from RFID?: A Case for Federal
Legislation', Duke Journal of Law and Technology Review, 3, 1.

Stockman, H (1948), 'Communication by Means of Reflected Power', Proceedings of the IRE, <http://www.rfidjournal.com/article/articleview/1338/2/129/> , 1196-1204.