YEARLY LEGAL REPORT ON UBIQUITOUS NETWORKS AND P2P NETWORKS THROUGH THE COPYRIGHT LENS.

María J. Iglesias[1] and Ana Isabel Cerezo Domínguez[2]
[1]Centre de Recherche Informatique et Droit FUNDP,
Head of the Intellectual Property Unit
e-mail maria-jose.iglesias@fundp.ac.be
[2] Universidad de Málaga,
Profesora Titular de Derecho Penal

October 8, 2009

Contents

1 YEARLY LEGAL REPORT ON UBIQUITOUS NETWORKS. 2

1.1 Introduction 2

1.2 Some Legal Implications Concerning The Infringement Of The Right To Privacy And Data Protection 3

1.2.1 Identification and profiling of a person 4

1.2.2 Unnoticed remote reading without line-of-sight 4

1.3 Legal Instruments On The Implementation Of Privacy And Data Protection Principles In Applications Supported By Radio- Frequency Identification 4

1.3.1 Applicability of existing privacy legislation 4

1.3.2 Enacting specific provisions on RFID 6

1.3.3 New EU recommendations 7

2 P2P NETWORKS THROUGHT THE COPYRIGHT LENS. 10

2.1 Abstract 10

2.2 Introduction 10

2.3 Legal framework. 11

2.4 P2P networks case law 11

Chapter 1

YEARLY LEGAL REPORT ON UBIQUITOUS NETWORKS.

by Ana Isabel Cerezo Domínguez

1.1 Introduction

The term Ubiquitous computing is attributed to Mark Weiser in a Scientific American article he wrote in 1991 [4]. Weisers vision focuses on a digital technology that is interactive, non-obtrusive and pervasive. His concern was that interfaces are too demanding of human attention. The increasing availability of smaller and smarter digital technology gives us useful access to invoke and receive services, anywhere and anytime. The concept of ubiquitous computing is human-centred - it centres on technology becoming invisible to, but yet readily accessible to humans.

Given the multi-disciplinary nature of Ubiquitous computing topic, this report is going to focus on legal aspects of RFID, the only one area of ubiquitous computing with some legislation.

Radio frequency identification (RFID) marks a new development in the information society where objects equipped with microelectronics that can process data automatically will increasingly become an integral part of every day life. RFID is progressively becoming more common, and hence a part of individuals' lives in a variety of domains such as logistics, healthcare, public transport, the retail trade, in particular for improved product safety and faster product recalls, entertainment, work, road toll management, luggage management, and travel

documents [2].

RFID technology has the potential to become a new motor for growth and jobs and thus make a powerful contribution to the Lisbon Strategy[1], as it holds great promise in economic terms, where it can bring about new business opportunities, cost reduction and increased efficiency, in particular in tackling counterfeiting and in managing e-waste, hazardous materials, and the recycling of products at their end of life. RFID technology enables the processing of data, including personal data, over short distances without physical contact or visible interaction between the reader or writer and the tag, such that this interaction can happen without the individual concerned being aware of it.

RFID technology applications hold the potential to process data relating to an identified or identifiable natural person, a natural person being identified directly or indirectly. They can process personal data stored on the tag such as a person's name, birth date or address or biometric data or data connecting a specific RFID item number to personal data stored elsewhere in the system. Furthermore, the potential exists for this technology to be used to monitor individuals through their possession of one or more items that contain an RFID item number.

Because of its potential to be both ubiquitous and practically invisible, particular attention to privacy and data protection issues is required in the deployment of RFID. Consequently, privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-by-design'). RFID will only be able to deliver its numerous economic and societal benefits if effective measures are in place to safeguard personal data protection, privacy and the associated ethical principles that are central to the debate on public acceptance of RFID.

1.2 Some Legal Implications Concerning The Infringement Of The Right To Privacy And Data Protection

RFIDs tag may be related to personal information. Data protection and the information self-determination is a precious fundamental right that should be protected from the technical development, if this proceeds without taking into account the conformity to main constitutional values and rights. It should be assured that the right to privacy and to data protection will not turn into a caprice of the individual but will still remain an obligation of the democratic society.

[1]The Lisbon Strategy, adopted by the European Council in 2000, demands an increase in the speed of innovation and in productivity to maintain Europe's competitiveness. RFID can make a significant contribution to this.

1.2.1 Identification and profiling of a person

RFID tags normally consist of a unique identification number. The use of the tag is to enable identifying and tracking every single item. Everyone who carries at least one so-tagged item is possible to get identified and tracked. RFID tags function as a unique identifier and the growing interoperability of the system makes allocating and tracking possible worldwide. Beyond that, the link-ability of RFID technology to other databases and their supersets-archives can facilitate the identification process. RFID information can be used independent from information of other sources. But the facileness of the combination of both turns it into a main threat to privacy. Once tagged objects are owned by persons, it is possible to be related to them. The ability of tracking objects might become an ability to track individuals. Using RFID technology retailers might track customers within their shops in order to create profiles of movement which can be used to improve marketing strategies. One should mention that this is possible only by connecting the information obtained by the tagged object that individuals carry with them and their customer or credit cards that they submit at the purchase point[1].

1.2.2 Unnoticed remote reading without line-of-sight

RFID tags can be read without line-of-sight and without overt evidence that they are being read. In addition their small size and the luck of need of energy supply make them appropriate to be installed hidden. The problem is that radio waves allow data to be processed over a given distance without any need for a direct line-of-sight link with the chip and without the data subject having to take an active part in the process. In other words, data processing can take place without the knowledge of the data subject. Any data on RFID transponders that have not been destroyed or deleted can be read by visible or even invisible readers. The unnoticed remote reading may indeed be used for various purposes without the knowledge of the person in question, for instance for unnoticed surveillance of workers, unnoticed profiling of one's consuming preferences etc[3].

1.3 Legal Instruments On The Implementation Of Privacy And Data Protection Principles In Applications Supported By Radio- Frequency Identification

1.3.1 Applicability of existing privacy legislation

A previous question is whether current regulatory frameworks, e.g. legislation and self-regulatory mechanisms for the protection of personal data, are applicable, adequate and efficient to address issues associated with RFID. In most cases,

existing privacy legislation, when it is technology neutral, seems applicable.

The rights and obligations concerning the protection of personal data and the free movement of such data are provided for by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications"). Both directives defend individuals against personal information processing adopting the Fair Information Practices with modifications. Therefore, controversial applications of RFID technology like association of data with personal identification or individual tracking are already regulated and involve a number of data protection obligations. The Directives grant data subjects a series of important rights including the right of access to personal data, know where data originated and the right to withhold permission to use data. In particular, location data requires consumer's permission prior to collecting or using information, without consent data should be anonymous. Especially, the 2002 Directive provides as follows:

Article 9 Location data other than traffic data:

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with then consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Is article 9 of Directive 2002/58/EC applicable? According to article 9 of the aforementioned Directive location data other than traffic data of subscribers or users of public communications networks or publicly available electronic communications services may be processed for the provision of a value added service only if they made anonymous or with the prior informed consent of the subscribers or users. The electronic communications service provider has thus the obligation to inform and obtain the consent of the data subjects. RFID technology may reveal or be primarily used for the localisation of persons. In this regard, it is to examine whether article 9 of Directive 2002/58/EC is applicable. The wording of this article and the scope of the Directive does not however provide for a direct applicability. Article 9 requires that a processing of personal location data is taking place within the context of a public communications network or a publicly available electronic communications service and, as a result addresses the obligations of the respective providers. RFID technology enables, on the other hand, a communication without the need of a publicly available network and the provision of such services nor involves respective providers.

Article 9 may be applicable only where the RFID technology is an additional feature of the terminal equipment of the subscriber or user which enables the provision of a value added service. For instance, an RFID enabled mobile phone may communicate subscriber's or user's data to third parties for the purpose of advertising when the owner of the RFID tagged mobilephone passes a certain point. To the extent the electronic communications service provider is transferring personal data to the third party, i.e. the name and number of the RFID tagged mobile phone owner, consent of the owner shall be prior obtained. Since RFID technology enables the location of persons, especially in an unnoticed and possibly very intrusive manner, it shall be further examined whether there is a need for a specific provision or whether, at least a uniform application of existing provisions may be achieved at EU level.

Finally, the principles laid down in Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity should be applied in the development of RFID applications. However, any of these legal instruments could solve satisfactory the problems involve RFID applications.

1.3.2 Enacting specific provisions on RFID

In 2006, the European Commission launched a public consultation (IP/06/289) on the development and use of smart chips (or radio Frequency identification technologies). The Commission communication of 31 May 2006 'A strategy for a secure information society 'Dialogue, partnership and empowerment' acknowledges that diversity, openness, interoperability, usability and competition are key drivers for a secure information society, highlights the role of Member States and public administrations in improving awareness and in promoting good security practices, and invites private-sector stakeholders to take initiatives to work towards affordable security certification schemes for products, processes

and services addressing EU-specific needs, in particular with respect to privacy.

Based on this, it then adopted a Communication in march 15th 2007 (IP/07/332) called "Radio frequency identification (RFID) in Europe: steps towards a policy framework". The document proposes a series of steps in order to facilitate the implementation of RFID and includes the issuing of a recommendation on the implementation of privacy, health and environmental safeguards. The Council Resolution of 22 March 2007 on a strategy for a secure information society in Europe invites Member States to give due attention to the need to prevent and fight new and existing security threats to electronic communications networks.

The "OECD Police Guidance on Radio Frequency Identification" was published on the occasion of the OECD Ministerial Meeting on the Future of the Internet Economy that took place on Seoul on 17-18 June 2008. This report contains policy and practical guidance principles to enhance business and consumer benefits from the use of RFID while proactively taking into account information security and privacy issues. It is supported by a report on economic aspects of RFID that reviews major fields of applications, economic impacts and country initiatives, as well as a report that analyses information security and privacy challenges and possible measures and safeguards to address them.

In December 2008, CEN, CENELEC, and ETSI (ESOs) received mandate M/436 on "Information and Communication Technologies applied to Radio Frequency Identification (RFID) and systems". The mandate addresses data protection, privacy and information security aspects of RFID. It complements the existing legal framework. Furthermore, the mandate invites the ESOs to develop sector specific RFID implementation guidelines, as complementary documents.

1.3.3 New EU recommendations

Finally, the European Commission has adopted on may 12th 2009 a set of recommendations to make sure that everyone involved in the design or operation of technology using smart chips respects the individuals fundamental right to privacy and data protection. These recommendations were elaborated by consulting all stakeholders from both the supplying and using industries, standardisation bodies, consumers organisations, civil society groups, and trade unions, responds to these expectations and seeks to create a level-playing field for the European industry while respecting individuals privacy.

The commission laid out the following principles for protecting privacy and data protection in their use:

Privacy and data protection impact assessment An assessment of the privacy and data protection impacts carried by the operator prior to the implementation of an RFID application will provide the information required for appropriate protective measures. Such measures will need to be monitored and reviewed throughout the lifetime of the RFID application. Companies and public authorities should conduct privacy and data impact assessments before using smarts chips. These assessments, reviewed

by national data protection authorities, should ensure that personal data is secure and well protected. Member States should ensure that these operators:

1. conduct an assessment of the implication of the application implementation for the protection of personal data and privacy, including whether the application could be used to monitor an individual. The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application.
2. take appropriate technical and organisational measures to ensure the protection of personal data and privacy.
3. Designate a person or group of persons responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures to ensure the protection of personal data and privacy.
4. Make available the assessment to the competent authority at least six weeks before the deployment of the applications.
5. Once the framework for privacy and data protection impact assessment is available implement the above provisions in accordance with it.

Information security Member States should support the Commission in identifying those applications that might raise information security threats with implications for the general public. For such applications, Member States should ensure that operators, together with national competent authorities and civil society organizations, develop new schemes, or apply existing schemes, such a certification or operator self-assessment, in order to demonstrate that an appropriate level of information security and protection of privacy is established in relation to the assessed risks.

Information and transparency on RFID use Member States should ensure that operators develop and publish a concise, accurate and easy to understand information policy for each of their applications. The policy should at least include:

1. the identity and address of the operators;
2. the purpose of the application;
3. a summary of the privacy and data protection impact assessment;
4. the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.

Companies or public authorities using smart chips should give consumers clear and simple information so that they understand if their personal data will be used, the type of collected data (such as name, address or date of

birth) and for what purpose. They should also provide clear labeling to identify the devices that "read" the information stored in smart chips, and provide a contact point for citizens to obtain more information.

RFID applications used in the retail trade Retail associations and organisations should promote consumer awareness on products containing smart chips through a common European sign to indicate whenever a smart chip is used by a product.

Consumers should be in control whether products they buy in shops use smart chips or not. When consumers buy products with smart chips, these should be desactivated automatically, immediately and free-of-charge at the point of sale, unless the consumer explicitly opts-in-by asking to keep the chip operational. Exceptions can be granted to avoid unnecessary burden on retailers, for example, but only after an assessment of the chip's impact on privacy.

Awareness raising actions Member States in collaboration with industry, the Commission and other stakeholders, should take appropriate measures to:

1. inform and raise awareness among public authorities and companies, in particular SMEs, of the potential benefits and risks associated with the use of RFID technology. Specific attention should be given to information security and privacy aspects.
2. Identify and provide examples of good practice in the implementation of RFID application to inform and raise awareness among the general public.
3. Increase public awareness of RFID technology, its benefits, risks and implications of use, as a prerequisite for wider take-up of this technology.

Research and development Member States should cooperate with industry, relevant civil society stakeholders and the Commission to stimulate and support the introduction of the security and privacy by design principle at an early stage in the development of RFID applications.

Follow-up Member States have two years to inform the Commission on the steps they intend to take to make sure that the objectives of the Recommendation are met. Within three years, the Commission will report on the Recommendations implementation, including an analysis of its impact on companies and public authorities using smart chips as well as its impact on citizens.

Chapter 2

P2P NETWORKS THROUGHT THE COPYRIGHT LENS.

by Mara J. Iglesias.

2.1 Abstract

Publication of synthetic —*i.e.* simulated— data is an alternative to masking for statistical disclosure control of microdata. The idea is to randomly generate data with the constraint that certain statistics or internal relationships of the original dataset should be preserved. Several approaches for generating synthetic data files are described in this report. The pros and cons of synthetic data are discussed and some suggestions to Eurostat are made.

2.2 Introduction

Distribution of digital content may be done by different ways. From a legal point of view it should be distinguished between legal distribution ?based either on proprietary licences or on open licences?, and illegal distribution, when copyright protected digital content is distributed without the permission of the rightholders. From a technical point of view, distribution of digital content may be done through P2P networks. Although traditionally P2P networks have been used to illegal files sharing i.e. copyrighted films and music-, thanks to the implementation of DRMs, and to the agreements reached between the rightholders representatives and P2P software providers, they are being used more a more for commercial and licit distribution of digital contents. In the following pages

we will focus on the legal framework concerning the distribution of copyrighted files without the permission of right holders through peer to peer networks.

2.3 Legal framework.

Reproduction and making available of copyrighted works through P2P networks need the permission of the copyright holder, unless a limitation applies. One might argue that the distribution of copyrighted files through P2P systems may fall under the scope of the private copy exception contained in. art. 31.2 of the Spanish Copyright Law. It authorised the reproduction of a lawfully acquired copy of copyrighted work when it is done for private purpose of a natural person, provided the copy is not used for collective or gainful purposes. Since the used made under P2P networks implies a collective utilization of the work and affects not only to the reproduction right but also to communication right[1], the file sharing of digital files does not fit in the scope of this provision.

2.4 P2P networks case law

Thus, the legality of file sharing networks does not refer to the network or the software itself ?that can clearly serve to vey licit purposes?, but to the utilisation that users make through them, it means to the unauthorised distribution of copyrighted material. Having said that, there is case law where it has been considered that the responsible of the software has incurred in an illicit activity. The legal reasoning to found liability would depend on the technical characteristics of the P2P network

In US the two fundamental cases on file sharing jurisprudence clearly illustrates this difference. In the Napster case (2001)[2], it was considered that Napster, a centralised P2P network- was liable as a secondary infringer, under the so-called contributory and vicarious liability. Napster had engaged in personal conduct that encourages or assists the infringement" because it "knowingly encourages and assists the infringement of plaintiffs' copyrights." Vicarious liability was founded on the fact that Napster had "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities". This argument differs from the one in the Grokster case (2005)[3] a decentralised P2P system-, where, although the Supreme Court admitted that Grokster was capable of substantial non-infringing uses, secondarily liability was founded on the fact that Grokster induced its users to infringe. Australia case

[1] Art. 20 (2) (i) Spanish Copyright Law includes as a manifestation of the right of communication to the public the making available to the public of copyright works in such a way that members of the public may access them from a place and at a time individually chosen by them.

[2] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[3] MGM v. Grokster, 545 U.S. 913 (2005).

law shows a different argument. In the KazaA case (2005) [4], liability of the operator was based on its capacity to implement filtering systems to discourage and impede the sharing of copyrighted files. KazaA had been also judged in the Netherlands (2003) [5], where, on the contrary, the Supreme Court considered that KazaA could not technically make impossible the unlawful copyrighted content sharing and then might not be held liable for the actions committed by its users.

In Spain, there is no major case law on P2P networks. Most relevant decisions concern the activity of individual users or the provision of links to P2P software sites. A set of minor decisions has considered that the provision of these links does not constitute an infringement since there is no making available of copyrighted works[6] and the website holder does not pursue for profit purposes[7] or since the website manager had no knowledge of the illicit activity[8].

[4]Universal Music Holdings Australia Pty Ltd v Sharman License Holdings Ltd (2005) 220 ALRI.

[5]BUMA/STEMRA vs Kazaa BV, LJN number AN7253, -C02/186HR.

[6]Auto 25 July 2009, Juzgado de lo Mercantil nm. 7 de Barcelona,

[7]Auto 25 July 2009, Juzgado de lo Mercantil nm. 7 de Barcelona, Auto 17 June 2009, Juzgado de Instruccin nm. 3 de Alcoy, Auto 4 June 2008, Juzgado de Instruccin nm. 4 de Cartagena.

[8]Auto 27 May 2009, Juzgado de Instruccin nm 48 de Madrid.

Bibliography

[1] S. Garfinkel and A. Juels. Rfid privacy: An overview of problems and proposed solutions. In *IEEE Security Privacy*, pages 34–43. IEEE, 2005.

[2] Pablo Najera and Javier Lopez. Rfid: Technological issues and privacy concerns. In Taylor and Francis Group, editors, *On Digital Privacy: Theory, Technologies, and Practices*, pages 285–306. Auerbach Publications, December 2007.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita. Rfid privacy issues and technical challenges. In *Communications of the ACM*, volume 48, pages 66–71. September 2005.

[4] M. Weiser. The computer of the 21st century. pages 94–100,. September 1991.