Chapter V
RFID Technology and its Impact on Privacy:
Is Society One Step before the Disappearance of Personal Data Protection?

Tatiana-Eleni Sinodinou
Bar Office of Thessaloniki, Greece

ABSTRACT

The present chapter explores privacy issues posed by the use of RFID systems and applications. The existing legal framework for data protection is analyzed in order to discover how general privacy safeguarding principles should be applied in the case of RFIDs, with special focus on the main areas which are going to experience widespread use of such applications. The structure of the chapter is based on a chronological order which follows the consecutive phases of contact and interaction between the individual and the RFID tag. The implementation of a tag to a product or in the human body establishes the first point of contact of the individual with the RFID tag. This stage of data processing is examined in the first part of the chapter. In more particular, this part deals with the application of general principles of fair processing, such as information transparency, the debate about the necessity to require the prior consent of the individual (possible opt-in and opt-out solutions) and the precondition of a clearly defined purpose of the data processing. The symbiosis of the person with the tag is examined in the second part. Indeed, privacy concerns are equally significant during the phase of processing of personal information, even if processing is conducted lawfully, either based on the legal ground of the individual's consent or justified on another legal basis. The requirement of data quality and the obligation to secure the RFID system against unauthorized interceptions or alterations of data by third parties constitute essential guarantees of fair data processing. Privacy protection in the activation phase of the

tag is also ensured by the obligation to inform the tagged individual every time a reading takes place and by the right to verify the accuracy of the tag data, whether stored from the beginning or added at a later date. Finally, the last part of the chapter examines the legal regime of separation between the person and the tag. This phase refers to the termination of the processing either by act of the data subject or by act of the RFID system controller. The focus is given to the exercise of the right to object to the processing of personal data through RFID devices. In this context practical solutions, such as the "tag kill" or "tag sleep" command should be taken into consideration in order to the make the exercise of the right to object feasible.

INTRODUCTION

New technologies have introduced a dynamic dimension in the exercise of individual liberties. However, they constitute at the same time a possible source of dominance, injustice, control and manipulation of the individual (Fraussinet in: Lucas, Deveze & Fraussinet, 2001, p.1). Technological evolution leads to complex pervasive technological realities which demand a strong protection of privacy. One of the most pertinent examples of new quasi-invisible forms of intrusion to privacy is the extended use of RFID systems.

RFID technology is based on the use of smart tags[1] which store and emit data through radiofrequencies by the means of miniscule antennas. The data and other information stored on the tag are received by a transceiver (reader)[2], which is also equipped with an antenna. Antennas are the conduits between the tag and the reader, which controls the system's data collection and communication (Flint, 2006). The salient features of this technology are that they permit the attachment of a unique identifier and other information – using a micro-chip – to any object, animal or even a person, and the reading of this information through a wireless device ("Radio Frequency Identification (RFID) in Europe: steps towards a policy framework", 2007).

The central idea is to give a unique identity to every "object", one which contains a smart tag, which can be transmitted to the reader ("Working document on data protection issues related to RFID technology", 2005).

This technology was first used on a large scale by the Royal Air Force during World War II to track enemy aircraft (*Identify Friend or Foe System*) (Lemoine, 2003). Nowadays, the commercial and social applications of RFID smart devices are limitless (Reid, 2007). The use of RFID technology can facilitate various activities in many sectors, such as in transports, in product distribution, in the retail sector, in the pharmaceutical industry, in healthcare services[3], logistics, the fight against counterfeiting[4], in aviation, in the automobile industry or in general every time it is necessary to control access ("Working document on data protection issues related to RFID technology", 2005).

From a technological point of view, there are two types of RFID tags: the passive and the active tags. Passive tags do not have an internal battery and cannot transmit data unless a reader activates them. On the contrary, active tags have an internal battery which permits the tag to emit the stored data but also to be rewritten and to store new data. Active tags offer more possibilities of data processing and are considered to be more privacy intrusive than passive tags.

RFID systems raise privacy and consumer protection concerns if they permit the identification of individuals. While the person's name is the most common feature of identification, identification can take place by use of other elements, such as