

## Chapter 7.1

# The Ethical Debate Surrounding RFID

**Stephanie Etter**

*Mount Aloysius College, USA*

**Patricia G. Phillips**

*Duquesne University, USA*

**Ashli M. Molinero**

*Robert Morris University, USA*

**Susan J. Nestor**

*Robert Morris University, USA*

**Keith LeDonne**

*Robert Morris University, USA*

### RFID TECHNOLOGY

Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity of an object or person wirelessly using radio waves (RFID Journal, 2005). It falls under the broad category of automatic identification technologies. RFID tags, in the simplest of terms, are “intelligent chips that can be embedded in or attached to a product to transmit descriptive data” (Gelinas, Sutton, & Fedorowicz, 2004, p. 6). According to the online *RFID Journal* (2005), there are several methods of identifying objects using RFID, including the most common of storing a serial number that identifies a product on a

microchip that is attached to an RFID tag. RFID is not a new technology, but it has only recently been in the spotlight as more businesses are receiving press for putting the technology to work in their supply chains.

RFID tag technology is sometimes associated with the term electronic product code (EPC). An EPC uniquely identifies objects in a supply chain. According to EPCGlobal, “EPC is divided into numbers that identify the manufacturer and product type. The EPC uses an extra set of digits, a serial number, to identify unique items.” The EPC number is placed on a tag composed of a silicon chip and an antenna, which is then attached to an item. Using RFID, a tag communicates its number

to a reader (EPCGlobal, 2005). In broad terms, RFID tags are placed into one of two categories: active or passive. According to the Association for Automatic Identification and Mobility (AIM, 2005), active RFID tags are powered by an internal battery and are typically designated as read-write tags. When a tag has read-write capabilities, the tag data can be modified. Passive tags, according to AIM, operate without a power source and obtain operating power from the tag reader. Passive tags are typically read-only tags, having only read-only memory. Active tags generally have a longer read range than passive tags.

RFID development dates back, according to some accounts, to the 1940s work of Harry Stockman who discussed the possibility of communication by means of reflected power. Stockman at that point was early in the exploration and “admitted that more needed to be done in solving the basic problems of reflected-power communication before the application could be useful” (Landt & Catlin, 2001). According to the *RFID Journal*, RFID’s early applications can be found during World War II when it was used by the military in airplanes, through the assistance of radar, to identify friend or foe (IFF).

Two decades later the first commercial use of RFID-related technology was electronic article surveillance (EAS), which was designed to help in theft prevention. These systems often used 1-bit tags that could be produced cheaply. Only the presence or absence of the tag could be detected, which provided effective anti-theft measures (Landt & Catlin, 2001).

Commercial applications expanded in the 1980s across the world, although not everyone had the same RFID applications in mind. The United States found the greatest applications for RFID to be in the areas of transportation, personnel access, and to a lesser extent, animal tracking. “In Europe, the greatest interests were for short-range systems for animals, industrial and business applications, though toll roads in Italy, France, Spain, Portugal,

and Norway were equipped with RFID” (Landt & Catlin, 2001).

Today we see RFID in use in toll collection, tracing livestock movements, and tracking freight (Jones, Clarke-Hill, Comfort, Hillier, & Shears, 2005). While not a new technology, the use of RFID is slowly gaining momentum for widespread application, with RFID technology being used in industries such as retail, banking, transportation, manufacturing, and healthcare.

## **PRIVACY DEBATE**

The two main controversies regarding the use of RFID are privacy and security. While advances in technology can address the security issues related to RFID, the ethical debate surrounding privacy is not as easily solved. As RFID technology becomes mainstream, its privacy protection challenges are becoming the topic of debate between technologists, consumer activists, academics, and government agencies. Yoshida (2005) reports that there is a “polarizing force tugging at the technology: the government and industry groups advocating RFID’s adoptions, and the civil libertarians concerned about its potential abuse.” The main question is, will this technology lead to situations where confidential information can be improperly disclosed? A representative from the UK’s Department of Trade and Industry warned, “RFID tags could be used to monitor people as well as merchandise. As the use of RFID spreads, privacy issues must be weighed in the context of societal consent” (Yoshida, 2005).

RFID is not the first technology to spur a privacy debate. While technologies like RFID are not necessary for the invasion of privacy, they have made new privacy threats possible and old privacy threats more powerful. Based on IT ethics literature, there are three key aspects to privacy that computer technology tends to threaten (Baase, 2003):

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/ethical-debate-surrounding-rfid/37854](http://www.igi-global.com/chapter/ethical-debate-surrounding-rfid/37854)

## Related Content

---

### Ubiquitous and Pervasive Application Design

M. Bakhouya and J. Gaber (2010). *Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications* (pp. 182-190).

[www.irma-international.org/chapter/ubiquitous-pervasive-application-design/37787](http://www.irma-international.org/chapter/ubiquitous-pervasive-application-design/37787)

### Biometrical Identification as a Challenge for Legislation: The Finnish Case

Reima Suomi, Tuomas Aho, Tom Björkroth and Aki Koponen (2009). *Risk Assessment and Management in Pervasive Computing: Operational, Legal, Ethical, and Financial Perspectives* (pp. 233-245).

[www.irma-international.org/chapter/biometrical-identification-challenge-legislation/28458](http://www.irma-international.org/chapter/biometrical-identification-challenge-legislation/28458)

### Security and Privacy in RFID Based Wireless Networks

Denis Trcek (2010). *Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications* (pp. 1386-1395).

[www.irma-international.org/chapter/security-privacy-rfid-based-wireless/37857](http://www.irma-international.org/chapter/security-privacy-rfid-based-wireless/37857)

### Adaptive Resource and Service Management in a Mobile-Enabled Environment

Claudia Raibulet (2010). *Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications* (pp. 1527-1548).

[www.irma-international.org/chapter/adaptive-resource-service-management-mobile/37866](http://www.irma-international.org/chapter/adaptive-resource-service-management-mobile/37866)

### Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information

Glorin Sebastian (2023). *International Journal of Security and Privacy in Pervasive Computing* (pp. 1-14).

[www.irma-international.org/article/privacy-and-data-protection-in-chatgpt-and-other-ai-chatbots/325475](http://www.irma-international.org/article/privacy-and-data-protection-in-chatgpt-and-other-ai-chatbots/325475)