Chapter 69
Consumers' Perceptions of Item-Level RFID Use in FMCG:
A Balanced Perspective of Benefits and Risks

Wesley Kukard
Auckland University of Technology, New Zealand

Lincoln Wood
The University of Auckland, New Zealand & Curtin University, Australia

ABSTRACT

This research explores how perceived consumer benefits affect the perceived privacy risks from implementation of Radio Frequency Identification (RFID) tags at an item-level in the Fast Moving Consumer Goods (FMCG) industry. Two new categories measure the benefits and risks: in-store and after-sales. These specific categories allow the respondents' willingness to accept RFID to be evaluated using a quantitative survey focused on the primary household grocery purchasers within the USA. The results suggest differences in perceptions of the in-store and after-sales risks and benefits of RFID use. While consumers are aware of privacy risks while using RFID technology, they would be willing to use the technology if sufficient benefits are available. This research moves the discussion away from a focus on consumer privacy issues to a balanced privacy/benefits approach for consumers and how that might affect their technology acceptance, suggesting that careful management of consumer benefits might allow FMCG firms to introduce RFID technology to support their global supply chains.

INTRODUCTION

As technology moves forward, we will see a future where all devices are connected to the Internet – a 'connected future' (Burrus, 2014). While the concept of a connected future remains in its infancy now, it is built on an expectation of the future and our way of life. In much in the same way social media has evolved to become a fundamental part of day-to-day life, the 'Internet of Things' (IoT) paradigm will soon

become embedded as a part of life over the globe, as "[b]y 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more" (National Intelligence Council, 2008, p. v.). RFID technology has become synonymous with the IoT paradigm, as the technology uses wireless and uniquely identifiable chips that are low cost, easy to produce, and easy to integrate into existing manufacturing processes. Since RFID gained popularity in the early 2000s, there has been a focus to create an industry standard for RFID's Electronic Product Code (EPC). A standard would improve visibility, traceability, awareness of the chips status and current location in the supply chain – these are all key components on the path to the full deployment of the IoT vision (Atzori, Iera, & Morabito, 2010). Combined, these components provide valuable supply chain information.

To understand the implications for global firms shifting their products and services in recognition of the IoT, we focus our attention on implementation opportunities in the FMCG industry. Due to the large number of good and the way that FMCG touches the lives of everyone, this is likely where the IoT will become a part of everyday life. Nine of the top ten FMCG multinationals are based either in Europe or the United States (Statista, 2014), their reach is truly global, and their decisions impact the lives of billions of people on a daily basis. FMCG products typically have a short life cycle; item-level RFID-tags are the only feasible option to integrate FMCG products into a global IoT network.

To understand how global FMCG companies will be able to establish an IoT using RFID technology, we must first understand the role of consumer acceptance of this technology. Given the United States and European base for the global FMCG firms, we assume that the appropriate technology will be first tested and deployed in such wealthier and more technology-savvy marketplaces. Therefore, understanding whether consumers in these home markets will accept and adopt the RFID technology becomes central to whether or not the FMCG firms can effectively establish an IoT. Then, as the technology is adopted around the globe, the FMCG firms will be effectively positioned to manage the global flows of products and information. All these commercial benefits, however, require FMCG firms to understand and be effective custodians of consumer data in a way that alleviates any consumer concerns about information privacy.

Consumers are more likely to be accepting of a technology that can drive benefits (Östman, 2013), without undue risk to themselves. Some retail outlets now use fast self-checkouts or are eliminating checkouts altogether through the use of RFID; while these changes represent a cost saving to the retailer (Prater, Frazier, & Reyes, 2005), the consumer would gain only a minor time-saving as a benefit. What is required are some substantial after-sales benefits for consumers. However, most after-sales benefits require RFID tags to remain active after purchase, potentially opening up consumers to unauthorized data collection within their home. Smith, Milberg, and Burke (1996) identify four dimensions of information privacy: collection, secondary unauthorized access (internal/external), improper access, and errors.

This research is important as it focuses on consumers' perceptions of risks and benefits of RFID use, in contrast to industrial perspective or a focus only on perceived risks. While much research has focused on industrial adoption and acceptance of RFID, this leaves open the question: At what point does household technology overstep the privacy boundary? An ever increasing amount of consumer electronic devices being integrated with various sensors, cameras, microphones and internet nodes to upload and use the collected data. There is a strong connection between IoT and RFID (Anderseck et al., 2012), as RFID is low-cost and uniquely identifiable, and can, therefore, keep track of lower cost disposable items, turning them from everyday grocery items, into smart grocery items. However, most research on RFID in the retail sector focuses on risks. There has been limited focus on benefits, despite growing consumer acceptance of related wireless technologies like NFC due to benefits. Smith et al.

Related Content

A Generic Self-Evolving Multi-Agent Defense Approach Against Cyber Attacks

Stephen Mugisha Akandwanahoand Irene Govender (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 210-226).

www.irma-international.org/chapter/a-generic-self-evolving-multi-agent-defense-approach-against-cyber-attacks/228728

Prolegomena for Cyborgoethics

(2022). *Philosophical Issues of Human Cyborgization and the Necessity of Prolegomena on Cyborg Ethics (pp. 287-306).*

www.irma-international.org/chapter/prolegomena-for-cyborgoethics/291954

Deciphering the Myth About Non-Compliance and Its Impact on Cyber Security and Safety

Kwasi Danso Dankwa (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 59-72).*

www.irma-international.org/chapter/deciphering-the-myth-about-non-compliance-and-its-impact-on-cyber-security-and-safety/253662

Penetration Testing Building Blocks

Abhijeet Kumar (2023). *Perspectives on Ethical Hacking and Penetration Testing (pp. 255-279).*

www.irma-international.org/chapter/penetration-testing-building-blocks/330268

Dimensions of Privacy Concerns Amongst Online Buyers in India

Tinu Jainand Prashant Mishra (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1214-1229).

www.irma-international.org/chapter/dimensions-of-privacy-concerns-amongst-online-buyers-in-india/228779