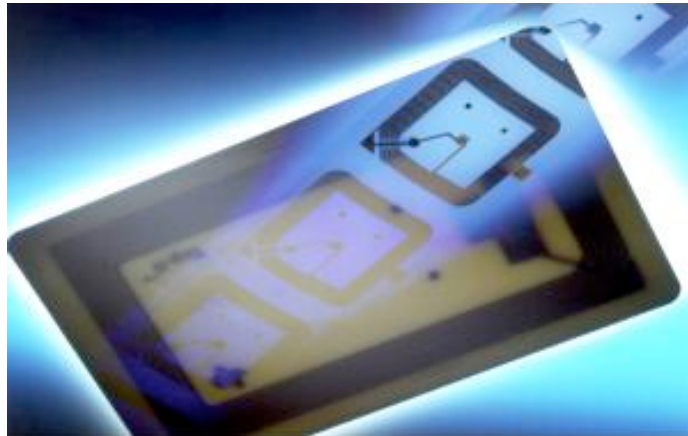

Policy in Socio-Technical Transition

The Case of Consumer Privacy Protection for Radio Frequency Identification (RFID) in Retail



Author: Victor Wanningen

Student registration number: 0008281

Study: Master Philosophy of Science Technology and Society (PSTS)

Course: Master's Thesis STS (course code: 162290)

Graduation Committee:

Prof. dr. S. Kuhlmann, Dr. ir. E.C.J. van Oost, and Dr. H. Klein

Date: 25 June 2009

Abstract

This study aims to understand emerging regulation in the regulatory dimension of socio-technical transition. Thereto, the Multi-Level Perspective (MLP) on socio-technical transition is applied in an experimental fashion to a ‘moving target’, i.e. a contemporary case study. In addition, the MLP is employed in a ‘prospective fashion’ by matching the empirical patterns with one of its five socio-technical transition pathways. In doing so, the MLP is symbiotically combined with the Governance Perspective (GP) into the hybrid MLP-GP analytical framework. The GP conceptualizes emerging regulation in terms of the governance dynamics of an emerging governance regime, i.e. multi-actor and multi-tier policy processes yielding policy outcomes. The hybrid MLP-GP analytical framework is applied to the empirical research field by conducting a governance case study of the emerging regulation for consumer privacy protection of Radio Frequency Identification (RFID). Currently, in the European retail sector experiments with the application of RFID on consumer products in the business-to-consumer (B2C) domain are conducted in RFID pilot projects in the technological niche. The RFID governance case study enables to get insights into the emerging regulation for consumer privacy protection of RFID in this new application domain. The observed empirical patterns were matched with the ‘transformation pathway’ as one of the five socio-technical transition pathways of the MLP. Finally, the *policy niche* as an analytical concept is introduced to conceptualize the emerging regulatory capability to accommodate an emerging technology in the ‘technological niche – socio-technical regime interaction’ of the ‘transformation pathway’.

Key words: RFID pilot project, technological niche, socio-technical regime transition, socio-technical transformation pathway, policy, regulation, governance regime, governance dynamics, policy niche

Table of contents

Abstract	3
Preface	7
1. Introduction	9
1.1 The RFID technology.....	9
1.2 Policy concerns.....	10
1.3 Practically relevant, puzzling, and theoretically relevant.....	10
1.4 Research scope	11
1.5 Research objective	11
1.6 Empirical research questions.....	11
1.7 Overview report chapters.....	12
2. Conceptualization	13
2.1 A hybrid analytical framework.....	13
2.2 The Multi-Level Perspective (MLP) on socio-technical transition.....	14
2.3 The Governance Perspective (GP).....	23
2.4 Operationalization of the MLP-GP hybrid analytical framework.....	27
2.5 Conceptual-laden research questions	29
3. Research methodology and strategy	30
3.1 An RFID governance case study	30
3.2 Criteria for the execution of the RFID governance case study.....	31
3.3 Scope and execution of the RFID governance case study	31
3.4 Analysis and reporting	37
4. RFID governance case study part one – The need for a RFID-specific regulatory capability for consumer privacy protection in retail	38
4.1 Introduction.....	38
4.2 The global Electronic Product Code (EPC) standards suite (Q1+Q2).....	39
4.3 EPC/RFID consumer privacy controversies in the EU and the US (Q2+Q4).....	44
4.4 The METRO Group Future Store Initiative phase one (METRO 1) (Q1-Q4)	47
4.5 The voluntary EPC industry self-regulation initiative (Q2+Q4)	54
4.6 Conclusion	57

5. RFID governance case study part two – The emerging RFID-specific regulatory capability for consumer privacy protection in retail	60
5.1 Introduction	60
5.2 Regional tier of the governance regime – Nordrhein-Westfalen (Q2-Q4).....	61
5.3 National tier of the governance regime – Federal Republic of Germany (Q2-Q4)	65
5.4 Transnational tier of the governance regime – European Union (EU) (Q2-Q4)	74
5.5 International tier of the governance regime – Transatlantic EU-US (Q2-Q4).....	82
5.6 Local tier of the governance regime revisited – The METRO Group Future Store Initiative phase two (METRO 2) (Q1-Q4).....	89
5.7 Conclusion	94
6. Discussion – Understanding the emerging RFID-specific regulatory capability in socio-technical transition	96
6.1 Different modes of governance (Q4).....	96
6.2 The socio-technical transformation pathway (Q5).....	98
6.3 Policy recommendation (Q6)	101
6.4 Conceptual contributions (Q7)	103
7. Philosophical reflection – Surveillance and privacy protection of RFID	105
7.1 The advanced global information society	105
7.2 Informational privacy and surveillance.....	106
7.3 RFID changes the nature of surveillance.....	107
7.4 The regulatory accommodation for RFID in the new mode of surveillance	108
8. Conclusion	109
8.1 The main findings	109
8.2 General reflection upon the RFID governance case study	110
8.3 Research recommendation for the empirical level.....	110
8.4 Research recommendation for the conceptual level.....	111
Acronyms.....	112
Bibliography	115
Appendices.....	124
Appendix A – The Interview Protocol	124

Preface

This report contains the master's thesis that I conducted within the master's program Philosophy of Science Technology and Society (PSTS) at the University of Twente located in Enschede in the Netherlands. The primary aim of the PSTS master's program is to study the meaning of science and technology in today's world. Within the master program, I took the Science Technology and Society (STS) studies specialization track. Within this track, I further specialized by participating in the specialization program issued by the PRIME network of excellence. PRIME stands for 'Policies of Research and Innovation in the Move towards a European Research Area'. PRIME is a collaborative, multidisciplinary, and international research program in which several European and an American research institute participates. Within the PRIME network, I visited the School of Public Policy (SPP) of the Georgia Institute of Technology located in Atlanta in the United States. At the SPP, I had the opportunity to do research for my master's thesis for a period of seven months. During my stay at the SPP, I had a great time, and therefore I want to thank everybody who directly or indirectly assisted me during the execution of my master's thesis.

Victor Wanningen, Enschede, June 2009

1. Introduction

'RFID will form the basis of better and safer healthcare, drastically improved supply chain management, low cost environmental monitoring for a cleaner, more sustainable future. We need a pro-active European approach so that we can benefit from the advantages of RFID while giving citizens, consumers and businesses choice, transparency and control.'

-- Viviane Reding, EU Commissioner for Information Society and Media¹

What is RFID and how can it benefit citizens, consumers, and business in the European Union (EU)? Why should the EU take a proactive approach in this matter? Well, this research aims to provide answers. It investigates the role of policy in technological innovation and specifically the application of the RFID technology in the supply chain management in retail.

1.1 The RFID technology

RFID is an emerging technology that enables the wireless identification, authentication, tracking and tracing of physical entities throughout a digital information system using Radio Frequencies (RF). A basic RFID system, see figure 1 below, consists of the following three components. Firstly, a RFID tag or transponder that contains a silicon microchip attached to a copper or aluminum antenna. Secondly, a RFID reader or interrogator that can remotely read the information stored on the microchip of the RFID tag using RF. Finally, the back-end information system in which the information read from the RFID tag by the reader receives its representation in a particular application context. RFID tags can be active or passive depending on their energy source. Active RFID tags have a battery as their energy source, whereas passive RFID tags generate their own energy from the electromagnetic energy emitted by the reader. Consequently, active and passive RFID tags work differently and have different properties such as reading distance, size, cost, durability, and functionality. RFID tags can be attached or embedded into, people, animals, and objects. RFID, therefore, has the potential to add value to any application context in which there is a need for physical entities to be identified, authenticated, tracked, or traced.

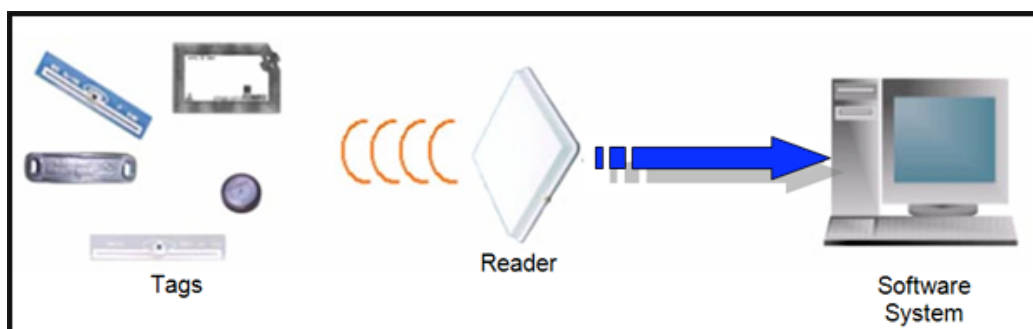


Figure 1 - The three basic building blocks of an RFID system (Bent, 2009)

¹ Quote Viviane Reding retrieved from: EC-networkRFID, 2009.

1.2 Policy concerns

In the EU, the European Commission (EC) promotes RFID as a beneficial future ubiquitous technology within their vision of the 'Internet of Things' (IoT). This vision holds that the physical world of objects and the virtual world of digital information get integrated when in the future RFID tagged objects are ubiquitous (EC-IoT, 2009). For the period between 2005 and 2010 as part of the Lisbon strategy, the EC propagates 'The European Information Society 2010 policy framework', i2010 for short. The core objective of i2010 is to make Europe the most competitive region in the world in the 'Information Age'. With the i2010, the EC puts forward a comprehensive and uniform European Information and Communication Technologies (ICTs) policy framework for the EU Member States to implement. The i2010 policy framework includes a RFID policy framework as well (EC-RFID-Policy, 2009). The EC propagates RFID as having the potential to automate various domains in society. Hereby, the EC envisions that RFID will add value to the EU's competitive edge within an ever-increasing competitive global economy. Next to this bright vision, RFID also has the potential for ubiquitous consumer surveillance by corporations, governments, and others – considered by many as a dark side. This as items equipped with RFID tags can be remotely read without consumers knowing it, hence causing an unprecedented threat to consumer privacy (CASPIAN, 2003).

1.3 Practically relevant, puzzling, and theoretically relevant

In the retail sector, field tests with the Electronic Product Code (EPC) stored on RFID transponders in the retail supply chain have started. The EPC is positioned as the promising digital successor of the European Article Number (EAN) and Universal Product Code (UPC) barcodes found on consumer products today. This new application domain of RFID has proven not to be free from problems. For instance, in 2004, the METRO Group, a big German retailer, had to abort a part of its RFID pilot project on consumer products due to consumer protests. Failing to notify the customers that RFID tags were embedded in the customer cards, this RFID pilot project of the METRO Group entered the history books as the most famously known consumer privacy controversy of RFID (Hof, 2007). In 2003, also in the UK the Tesco/Gillette pilot ended prematurely due to consumer protests. In 2003, Wal-Mart a big retailer in the United States (US) also conducted a RFID pilot project and had to rollback its operations due to consumer protests. In 2008, the METRO Group re-launched a RFID pilot project on consumer products. Although being closely monitored by various interest groups, this new RFID pilot project of the METRO Group does not report any consumer privacy issues so far. The rollout of RFID in retail, therefore, is not a simple and straightforward process, hence making it an intriguing object for investigation.

The EC's RFID policy framework aims at highlighting the positive and mitigating the potential negative consequences of RFID, as for instance manifested in the initial RFID pilot projects. However, there is something puzzling to the EC's RFID policy framework. Why is it that the EC promotes RFID regulation when at the same time it wants to promote competitiveness? One general conception that cumbersome regulation would hurt technological innovation and hence impede upon competitiveness does not apply here. It seems that the EC firmly holds the belief that well-structured regulation can actually enhance market competitiveness and create win-win situations among stakeholders. Furthermore, do the EC's proposed RFID regulations adequately address the social concerns of consumer privacy protection and hence pave the way for a smooth societal adoption of RFID?

Recent studies regarding (radical) technological innovation aim to better understand the process of socio-technical transition (Geels & Schot, 2007a). Geels and Schot (2007a) conceptualize transition in terms of socio-technical outcomes resulting from socio-technical

processes. Within this context, studying the role of regulation, in this case consumer privacy, that develops alongside technological innovation, in this case the RFID technology, will substantially contribute to understanding socio-technical transition that takes place in its societal context.

1.4 Research scope

As stated above the general scope of this research is policy in socio-technical transition, especially the regulatory dimension of socio-technological transition. More specifically, this study attempts to discuss the pivotal role of the consumer privacy regulatory dimension of the socio-technical transition of RFID. This as RFID is applied on consumer products in the retail sector, i.e. Consumer Product Item-Level Tagging (CPILT) in the front-end in-store Business-to-Consumer (B2C) application domain in retail. Because consumers do not interact with RFID in the back-end Business-to-Business (B2B) supply chain domain, this domain is kept in the background. Finally, this study is *temporally* bounded by the period between 2002 and 2009 and is *geographically* bounded by the EU and predominantly Germany.

1.5 Research objective

The main objective of this study is to *understand the policy outcomes as the result of the policy processes in the regulatory dimension of socio-technical transition*. This comes down to understanding the consumer privacy policy outcomes for RFID applied on consumer products in retail in terms of the associated policy processes. The policy processes are the socio-institutional dynamics of cooperating, competing, and contesting stakeholder organizations in connected multi-tier policy arenas. Concrete examples of consumer privacy policy outcomes are the ‘EPCglobal Guidelines for EPC on Consumer Products’, the ‘OECD Policy Guidance on RFID’, and the draft version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’. The inquiry regarding the interplay of negotiating stakeholder organizations is pivotal in understanding these regulatory outcomes for consumer privacy protection.

1.6 Empirical research questions

Following from the research objective, the two central empirical questions in this study read as follows.

Primary question;

‘How can we understand² the emerging consumer privacy regulatory outcomes for RFID in terms of the multi-tier and multi-actor regulatory processes in the regulatory dimension of socio-technical transition?’

Secondary questions;

‘What insights can be derived from the answers to the primary question, to formulate an outlook and a policy recommendation concerning the diffusion of RFID in the retail sector in the near future, and to formulate a conceptual contribution concerning socio-technical transition?’

² Since this study is positioned within the descriptive field of Science Technology and Society (STS) studies, the word ‘understand’ is used. As this research pursues to construct a bridge between STS and the normative field of Public Policy (PP), the PP scholar may substitute the word ‘understand’ with ‘explain’.

1.7 Overview report chapters

The outline of the analysis in this research report is as follows. Chapter 2 presents the conceptual framework that will structure the analysis in this study. The methodology and research strategy follows in chapter 3, as empirical data from the research field informs the analysis. Chapter 4 and chapter 5 present the case study of the emerging consumer privacy regulation that is centered on the RFID pilot projects of the METRO Group in the EU. Then chapter 6 will reflect upon the results of the case study in the light of the conceptual framework to assess the potential of RFID in the European retail sector. Accordingly, these insights will be drawn upon to formulate a policy recommendation and to formulate a conceptual contribution. Then chapter 7 presents a philosophical reflection upon surveillance and privacy protection of RFID in relation to the subject matter as presented in the previous chapters. The final chapter provides the summary and concluding remarks.

2. Conceptualization

2.1 A hybrid analytical framework

This chapter combines two analytical frameworks into one hybrid analytical framework to study the regulatory dimension of socio-technical transition. The Multi-Level Perspective (MLP) on socio-technical transition by Geels and Schot (2007a) is the first analytical framework and is discussed in section 2.2.³ The MLP serves to conceptualize technological innovation in terms of socio-technical transition to acknowledge its multi-faceted nature in its societal context. Subsequently, to open the ‘black box’ of the emerging regulations in the regulatory dimension of socio-technical transition, the MLP is combined with a second analytical framework in section 2.3. This is the Governance Perspective (GP) by Kuhlmann (2001, 2002, and 2003), Edler and Kuhlmann (2003), and Benz (2006). Then in section 2.4, the hybrid MLP-GP analytical framework is operationalized within the context of the research field. The regulatory dimension of socio-technical transition is fleshed out empirically by the emerging regulations for consumer privacy protection of RFID. This as RFID is applied on Consumer Product Item-Level Tagging (CPILT) in the in-store Business-to-Consumer (B2C) domain in European retail sector. Finally, section 2.5 presents the conceptual-laden research questions phrased in terms of the hybrid analytical framework.

³ There are two reasons why the Multi-Level Perspective (MLP) on socio-technical transition by Geels & Schot (2007a), as a Science Technology and Society (STS) studies framework, for a policy study is chosen. First, the policy dimension of RFID is interwoven with the technological dimension of RFID. The MLP provides a comprehensive framework for incorporating both the policy dimension and the technological dimension of RFID. Secondly, this study is carried out within the STS discipline. When carried out in the Public Policy (PP) discipline, the theory chapter would likely have drawn upon the theoretical frameworks discussed in: ‘Essence of Decision: explaining the Cuban Missile Crisis’ by Graham Allison (1971) and Graham Allison and Philip Zelikow (1999).

2.2 The Multi-Level Perspective (MLP) on socio-technical transition

The *first* analytical perspective is the Multi-Level Perspective (MLP) on socio-technical transition by Geels and Schot (2007a).⁴ The MLP is a multi-level, multi-actor, and multi-dimensional perspective on socio-technical transition. The essence of the MLP is that the multi-level, multi-actor, and multi-dimensional processes concerning a successful technological niche innovation, result in a transition from one socio-technical regime to another. In other words, the MLP enables to understand socio-technical transition in terms of socio-technical processes yielding socio-technical outcomes.

The next sections will examine the various facets of the MLP as summarized in figure 2 depicted below. Section 2.2.1 discusses each level of the MLP before zooming in on their interrelation. Section 2.2.2 discusses the socio-technical transition dynamics, followed by section 2.2.3 that discusses the possible so-called socio-technical transition pathways. Finally, section 2.2.4 discusses why the MLP needs to be supplemented with the GP as the second analytical framework.

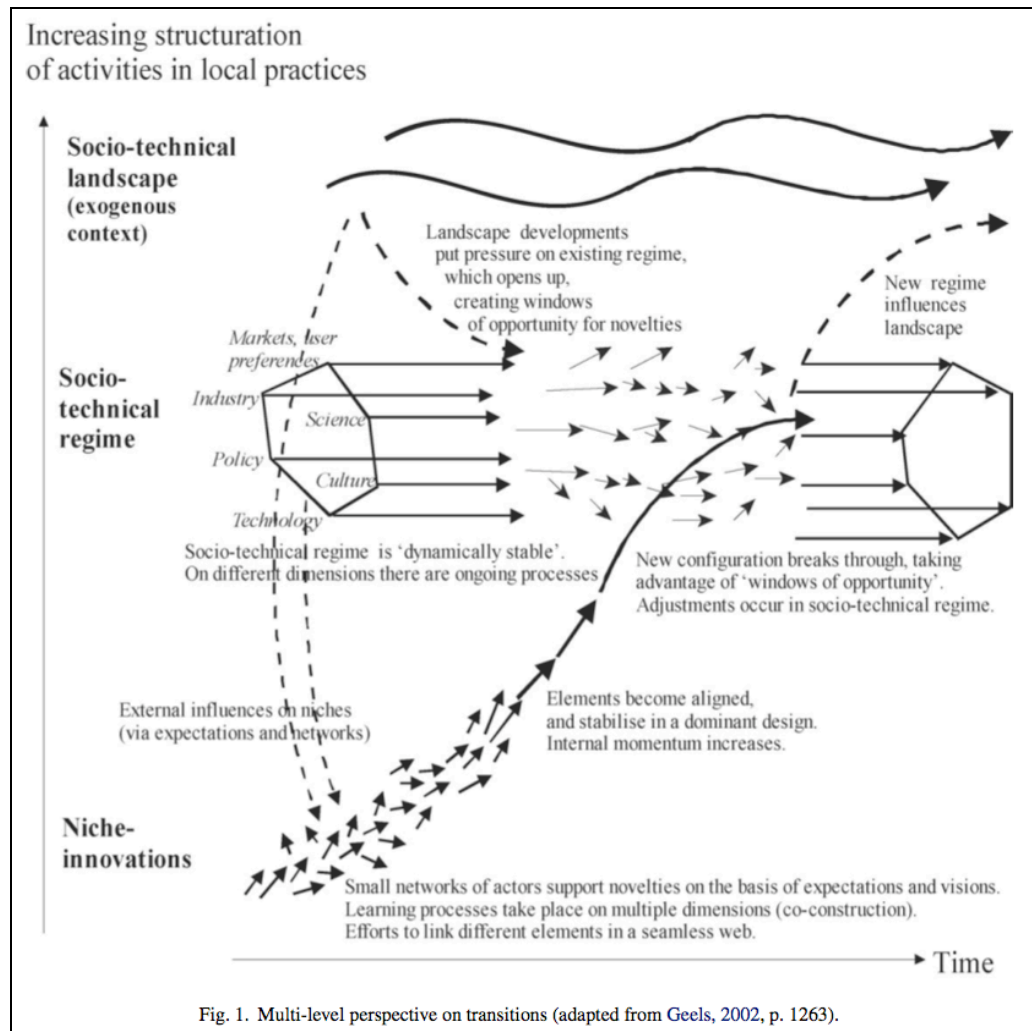


Figure 2 – Multi-Level Perspective (MLP) on socio-technical transition (Geels & Schot, 2007a: 401)

⁴ The MLP on socio-technical transition is an integrative perspective on technological innovation that draws upon disciplinary building blocks from: sociology of technology (SCOT (Pinch, Bijker), ANT (Latour, Callon), LTS (Hughes), expectations and strategic visions (Van Lente), domestication studies (Lie, Sorensen), business studies (radical product innovation (Christensen, Lynn), evolutionary economics (Nelson, Winter, Dosi), and institutional theory (Scott, Hodgson, North, Burns, Flams). The MLP came into being via Rip, Kemp, Schot and Geels; consult (Geels, 2006b: 166) for more information.

2.2.1 Three interrelated levels

The MLP on socio-technical transition consists out of three interrelated levels; these are the macro level, meso level, and micro level, see figure 2 above. Respectively, the following three sections will elaborate upon each of the three levels followed by how they are interrelated.

2.2.1.1 The macro level – socio-technical landscape

The first level of the MLP is the *macro level* or ‘socio-technical landscape level’. Here the focus lies on the dynamics regarding macro-economics, deep cultural patterns, and macro-political developments that make up the environment or context of socio-technical transition. The socio-technical landscape is the backdrop in which the networks of social groups or actors of the socio-technical regime and the technological niche reside and operate. The socio-technical landscape is able to exert pressure upon the socio-technical regime and the technological niche and hence plays an important role in stimulating a socio-technical transition.

Geels and Schot (2007a) employ the following definitions for the different socio-technical landscape pressures: ‘*Regular change* corresponds to environments that regularly experience a low intensity, gradual change. *Hyperturbulence* corresponds to environments that feature a high frequency of high-speed change in one dimension, e.g. ‘hyper-competition’. *Specific shock* corresponds to environmental changes that are rapid and high in intensity, come rarely, and are relatively narrow in scope. A *specific shock* may dissipate and disappear after a while, returning to base line, or it may lead to a structural stepwise change. *Disruptive change* corresponds to changes that occur infrequently, develop gradually, but have a high-intensity effect in one dimension. *Avalanche change* occurs very infrequently, but is of high intensity, of high speed, and simultaneously affects multiple dimensions of the environment. Avalanche change leads to permanent changes in the environment’ (Geels & Schot, 2007a: 404). The graphical equivalents of these socio-technical landscape pressures are presented in figure 3 below.

Frequency	Amplitude	Speed	Scope	Type of environmental change
Low	Low	Low	Low	Regular
High	Low	High	Low	Hyperturbulence
Low	High	High	Low	Specific shock
Low	High	Low	Low	Disruptive
Low	High	High	High	Avalanche

Fig. 4. Types of environmental change (based on Suarez and Oliva, 2005).

Figure 3 – Different socio-technical landscape pressures (Geels & Schot, 2007a: 404)

2.2.1.2 The meso level – socio-technical regime

The second level of the MLP is the *meso level* or ‘socio-technical regime level’. Here the focus lies on the dynamics regarding the organizational context, industry, knowledge institutions, and intermediate organizations of socio-technical transition. The ‘socio-technical regime’ consists of the distributed networks of actors and their institutions. These in combination with the interactions and alignment activities the actors have amongst each other are the *socio-institutional dynamics*. Figure 4 below provides a graphical representation of the socio-institutional dynamics articulated by the multi-actor network of the socio-technical regimes.

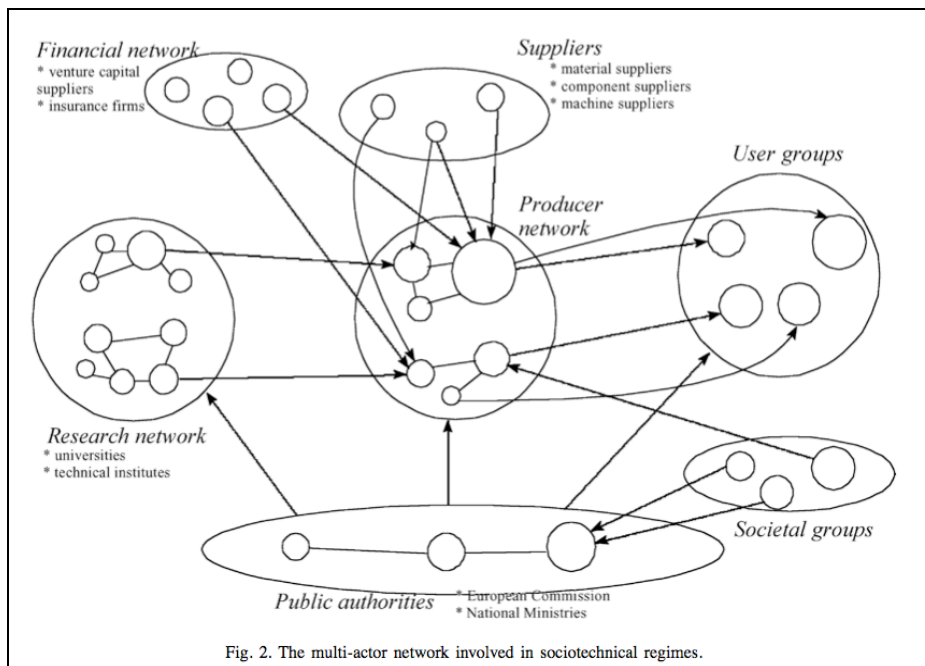


Figure 4 – The multi-actor network involved in socio-technical regimes (Geels, 2002: 1260)

The socio-technical regime is characterized by the alignment of ongoing co-constructive and co-evolutionary processes on multiple dimensions. According to Geels and Schot (2007a), these dimensions are the industry, markets and user preferences, science, culture (symbolic meaning of technology), technology and policy. Each of these dimensions is a regime as such, as figure 5 below indicates. The socio-technical regime makes up the totality of these heterogeneous regimes; hence, a socio-technical regime is appropriately called ‘a patchwork of regimes’ (figure 4 in: Geels, 2002: 1262).

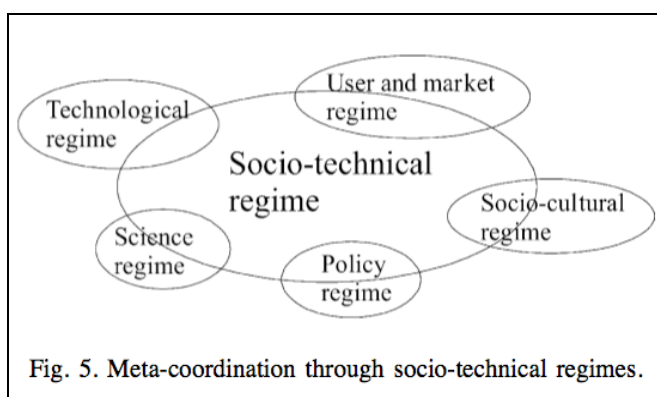


Figure 5 – Meta-coordination through socio-technical regimes (Geels, 2004: 905)

The notion of socio-technical regime and its relation to the technological niche and socio-technological landscape as employed by Geels and Schot (2007a) has its origin in the definition of a *technological regime* as provided by Rip and Kemp (1998: 340). They defined a technological regime as ‘the rule-set or grammar embedded in a complex engineering practices, production process technologies, product characteristics, skills and procedures, ways of handling relevant artifacts and persons, ways of defining problems; all of them embedded in institutions and infrastructures. Regimes are intermediaries between specific innovations as these are conceived, developed and introduced, and overall socio-technical landscapes.’ In addition, ‘Rip and Kemp (1998) add to the ‘rule-set’ or ‘grammar’ explicitly the policies and actions of other technology actors including public authorities’ (Kuhlmann, 2007: 6).

2.2.1.3 The micro level – technological niches

The third level of the MLP is the *micro level* or the ‘technological niche level’. Here the focus lies on the dynamics regarding the laboratories, businesses, engineering cultures and institutional settings of *emerging* radical technological innovations. In the technological niche existing practices and networks of actors shape, experiment, and test different variations of radical technological niche innovations. The activities take place in a real-life controlled and protected societal selection-environment, appropriately called an ‘incubation room’. In other words, a technological niche nurtures and protects emerging embryonic technological innovations against external influences such as the mainstream market selection. The networks of actors in a technological niche mutually create and accommodate a new technology and its societal selection-environment. The technological niche is the ‘controlled link’ between the co-constructed technological variation and its societal selection-environment. Technological niche innovations (innovations in a technological niche) therefore are *unstable emerging socio-technical configurations*, novelties or ‘novel configurations that work’ characterized by low performance (Geels & Schot, 2007a). Over time, a technological niche innovation can be successful and modify the incumbent socio-technical regime or it can fail in the unprotected societal selection-environment. The technological niche is influenced directly by the socio-technical regime and indirectly by the socio-technical landscape; see figure 6 below.

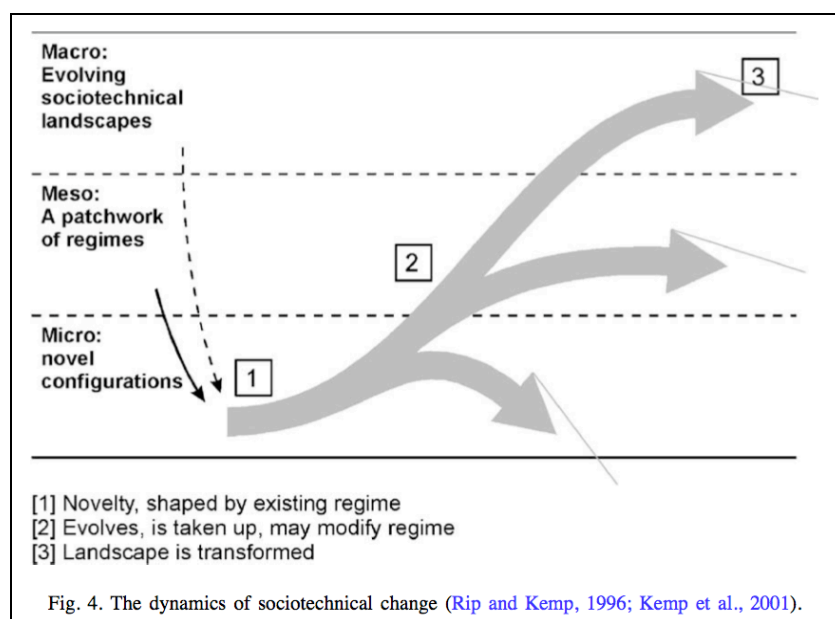


Figure 6 – The dynamics of socio-technical change (Geels, 2002: 1262)

Geels and Raven (2006) make a useful refinement to the conceptualization of a technological niche by making the ‘*global-local niche distinction*’. They define the *global niche-level* as the *emerging* community or organizational field of an emerging technological niche innovation. They define the *local niche-level* as the different real-life pilot projects and field tests that are being carried out in different local practices within the emerging community or organizational field. Figure 7 below provides a graphical representation of this distinction.

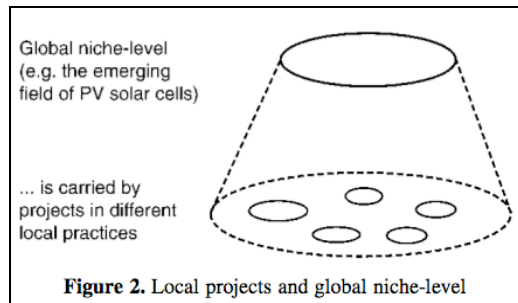


Figure 7 – Local projects and global niche-level (Geels & Raven, 2006: 378)

2.2.1.4 The interrelation between the macro level, meso level, and micro level

According to Geels and Schot (2007b, 2008), socio-technical regimes carry and store *rules* of how to use, produce, and regulate *incumbent technologies*. In technological niches, learning takes place of *how* to use, produce, and regulate *new technologies*. Socio-technical regimes and technological niches therefore bring together technology users, producers, and regulators. The socio-technological landscape is the environment that sustains the socio-technical regimes and the technological niches.

According to Geels and Schot (2007a), the MLP is a rule-based model for multi-level, multi-actor, and multi-dimensional action. The MLP considers rules and actors to be important factors in its *agency-structure dynamics*. To elucidate, the MLP focuses on the ‘rules of the game’, the processes of rule following, using, creation and alternation by the (organized and situated) actors concerning socio-technical transition. Pivotal in the *agency-structure dynamics* are the size and stability of the networks of actors and the stability of rules, as they happen to differ for each level of the MLP.

Following Geels and Schot (2007a), the socio-technical regimes and technological niches are inherently similar kinds of structures, but differ in terms of size and stability of their ‘sociological structuration’. Socio-technical regimes and technological niches are similar as they consist of communities of interacting social groups or actors in organizational fields. However, these are large and stable for the socio-technical regimes, and small and unstable for the technological niches.

According to Geels and Schot (2007a), the socio-technical regimes and technological niches are similar as they share certain rule sets that coordinate action, but differ in terms of the stability of these rules. On the one hand, rules can be *constraining*, as some actions are more legitimate than others are. On the other hand, rules can be *enabling*, as rules can enable convergence of actions, predictability, trust, and reliability. Geels and Schot (2007a) distinguish three types of rules sets that coordinate action: *regulative rules*, such as laws, standards and regulations, *normative rules*, such as role relationship, values and behavioral norms, and the *cognitive rules*, such as belief systems, innovation agendas, guiding principles, problem definitions and search heuristics. For the socio-technical regimes these regulative (formal), normative (behavioral) and cognitive (knowledge) rule sets are dynamically stable and well articulated whereas for technological niches they are unstable and under construction.

In respect to the socio-technological regimes and technological niches Geels and Schot (2007a) consider the socio-technical landscape to be different structure altogether. The

socio-technical landscape is the exogenous context that is characterized as the technical, physical, and material backdrop that sustains society. The socio-technical landscape therefore sustains action and makes some actions easier than others for the actors in the technological niches and socio-technical regimes. In respect to the technological niches and socio-technical regimes, the structure of the socio-technical landscape is the most stable of all the three levels and changes at the slowest rate.

2.2.2 Socio-technical transition

The MLP provides insights into how a socio-technical regime transition as the result of technological innovations in technological niches over time takes place. The breakthrough of (radical) technological innovations and their competition with the incumbent socio-technical regime, as the result of the interaction and the alignment processes between the macro level, meso level, and micro level, can result in a transition from the incumbent socio-technical regime to a new socio-technical regime. Geels and Schot summarize the essential workings of the MLP as follows. ‘The core notion of the MLP is that transitions come about through interactions between processes at the different levels: a) niche innovations build up internal momentum, through learning processes, price/performance improvements, and support from powerful groups, b) changes at the landscape level create pressure on the regime, c) destabilization of the regime creates windows of opportunity for niche innovation. The alignment of these processes enable the breakthrough of novelties in mainstream markets where they compete with the existing regime’ (Geels & Schot, 2007a: 400; Geels & Schot, 2008: 545).

When taking a closer look at the processes of the technological niche before a socio-technical regime transition takes place, a relation between the use of the new technology and the stability of its rules becomes apparent. When the nurtured and protected technological innovation in the technological niche has matured sufficiently its rules have done so either. As figure 8 below indicates, the technological niche then has the potential to grow and become a market niche, through a process that is called ‘niche-accumulation’ (Levinthal, 1998, cited in: Geels & Schot, 2007a). Once in the market niche, the technological innovation is ready to be exposed to the unprotected societal selection-environment and is able to compete with the incumbent regime in the marketplace.

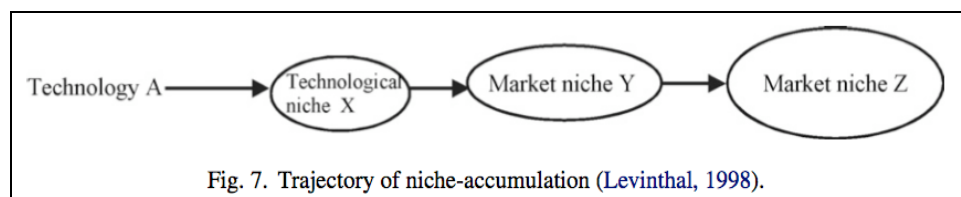


Fig. 7. Trajectory of niche-accumulation (Levinthal, 1998).

Figure 8 – Niche accumulation (Levinthal, 1998 cited in: Geels & Schot, 2007a)

As the new technology and hence its rules in the market niche are increasingly used in the organizational field, they become even more stable. Consequently, the market niche has the potential to topple the incumbent socio-technical regime by becoming the new socio-technical regime. The cycle and stages concerning the stability of rules and their usage in the organizational field in relation to the market niche and the socio-technical regime transition is depicted in figure 9 below.

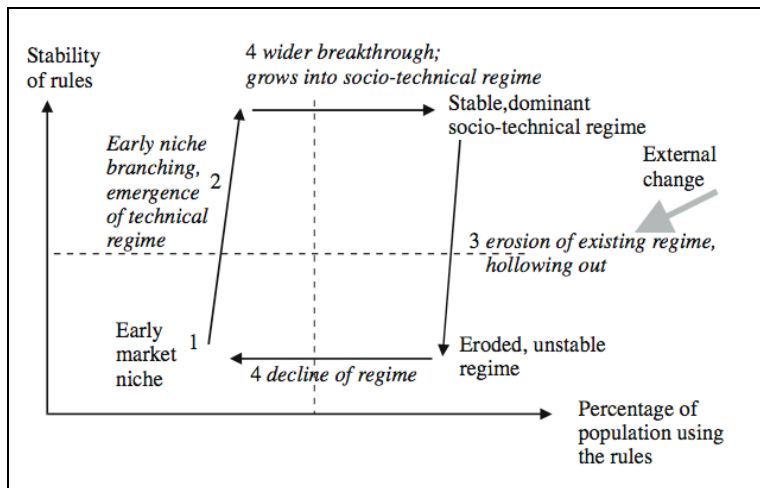


Figure 9 – Rules and their stability in socio-technical transition (Geels & Schot, 2007b: 614)

The next section provides insights into the transition processes from an incumbent socio-technical regime to a new socio-technical regime. This as a transition can take place via so-called socio-technical transition pathways that differ in timing and nature of the multi-level dynamics.

2.2.3 Socio-technical transition pathways

The MLP on socio-technical transition pursues to understand socio-technical transition in terms of multi-level, multi-actor, and multi-dimensional socio-technical processes yielding socio-technical outcomes. The following passage from Geels and Schot (2007a) makes this explicit. It also explains why the MLP on socio-technical transition does not explain with independent and dependent variables, but explains in terms of patterns that result from the interactions of the MLP. 'This incorporation of agency in transition pathways invites some further fundamental reflections on theory and agency. With its focus on interactions between niches, regimes and landscape, the MLP perspective provides narrative explanations. This does not imply storytelling or empiricism. The main point is that narrative explanations do not work with dependent and independent variables, but explain in terms of *patterns* that result from interactions. This is a specific type of theory, coined in the literature as process theory. Process theories explain outcomes as the result of temporal sequences of events, timing and conjunctures of event-chains. Situated groups make moves, undertake actions, and react to each other. Processes are understood as sequences of events that are enacted by situated actors' (Geels & Schot, 2007a: 414).

Based upon this notion, Geels and Schot (2007a) developed a typology of five possible socio-technical regime transition pathways. These provide insights into the processes and outcomes of socio-technical transition from an incumbent socio-technical regime to a new socio-technical regime. These five pathways differ in terms of *timing* and *nature* of the multi-level, multi-actor, and multi-dimensional interaction processes, consequently yielding different outcomes. In the transition pathways, niche innovations do not always have to be *competitive* to the incumbent regime but can also be *symbiotic* to the incumbent regime. A competitive niche innovation aims at replacing the incumbent regime. Conversely, a symbiotic niche innovation aims at becoming a competence-enhancing add-on to the incumbent regime to solve problems or to boost price and or performance. Furthermore, the socio-institutional dynamics differ in each of the five socio-technical transition pathways. Therefore Geels and Schot (2007a: 414) provide a characterization of the main actors and their (inter)actions in each of the five socio-technical transition pathways. The multi-level dynamics of the five socio-technical transition pathways are summarized in table 1 below.

Pathway name	Description
Pathway 0: Reproduction process	'If there is no external landscape pressure, then the regime remains dynamically stable and will reproduce itself'
Pathway 1: Transformation pathway	'If there is moderate landscape pressure ('disruptive change') at a moment when niche-innovations have <i>not</i> yet been sufficiently developed, then regime actors will respond <i>by modifying the direction of development paths and innovations activities</i> '
Pathway 2: De-alignment and re-alignment pathway	'If a landscape change is divergent, large and sudden ('avalanche change'), then increasing regime problems may cause regime actors to lose faith. This leads to de-alignment and erosion of the regime. If niche-innovations are <i>not</i> sufficiently developed, then there is no clear substitute. This creates space for the emergence of <i>multiple</i> niche-innovations that co-exist and compete for attention and resources. Eventually, one niche-innovation becomes dominant, forming the core for re-alignment of a new regime'
Pathway 3: Technological substitution pathway	'If there is much landscape pressure ('specific shock', 'avalanche change', 'disruptive change') at a moment when niche innovations have developed sufficiently, the latter will break through and replace the existing regime'
Pathway 4: Reconfiguration pathway	'Symbiotic innovations, which developed in niches, are initially adopted in the regime to solve local problems. They subsequently trigger further adjustments in the basic architecture of the regime'

Table 1 – Five socio-technical transition pathways (Geels & Schot, 2007a)

The MLP enables to conceptualize the socio-technical transition dynamics, i.e. socio-technical transition via a particular socio-technical transition pathway from an incumbent socio-technical regime to a new socio-technical regime, as the result of a successful niche innovation. To elucidate, the incumbent socio-technical regime carries and stores regulative (formal), normative (behavioral), and cognitive (knowledge) *rules* of how to *use, produce, and regulate* the *incumbent technology*. In technological niches, often in relation to the incumbent socio-technical regime, learning takes place by technology users, producers, and regulators concerning the regulative (formal), normative (behavioral), and cognitive (knowledge) rules of *how* to use, produce, and regulate the *new technology*. Once the rules in the technological niche become more stable and endorsed by a larger community, a transition, via a particular transition pathway, from the incumbent regime to the new regime can take place.

In this study, the MLP will serve to conceptualize the potential socio-technical transition, via a particular socio-technical transition pathway, from the incumbent EAN/UPC barcode regime to the new EPC/RFID regime in the European retail sector.

2.2.4 The need for a second analytical framework

This study aims at getting insights into the regulatory dimension of socio-technical transition that is fleshed out empirically by the emerging consumer privacy protection regulation for RFID applied on consumer products in the in-store B2C application domain in retail. The focus of this study therefore lies on emerging rules of how to regulate this new technology, i.e. predominantly on the emerging *regulative (formal) rules* embodied in *laws, standards, and regulations* concerning consumer privacy protection for RFID in its societal application domain. These emerging regulative (formal) rules are the result of the processes in which actors negotiate about these rules, i.e. the socio-institutional dynamics. The MLP because of its global perspective on socio-technical transition does not provide analytical tools to open the ‘black box’ of emerging regulation in its regulatory dimension. Hence, the MLP is combined with the Governance Perspective (GP) that provides analytical tools to reveal the emerging *regulative (formal) rules* of the regulatory dimension of socio-technical transition in terms of policy outcomes and its associated policy processes. In the following, section 2.3 discusses the GP and its integration with the MLP. Section 2.4 subsequently presents the operationalization of the hybrid MLP-GP analytical framework.

2.3 The Governance Perspective (GP)

In this study, the Governance Perspective (GP) will serve as an analytical perspective for guiding the empirical research of unpacking the emerging regulation in the regulatory dimension of socio-technical transition as conceptualized by the MLP. Governance is understood in terms of the definition of Kuhlmann (2007: 6) as 'a heuristic, borrowed from political science, denoting the dynamic interrelation of involved (mostly organized) actors, their resources, interests and power, fora for debate and arenas for negotiation between actors, rules of the game, and policy instruments applied.' In this section, section 2.3.1 and section 2.3.2 discuss the GP and section 2.3.3 integrates the GP with the MLP.

2.3.1 The Research and Innovation Policy Stakeholder's Arena

The main component of the Governance Perspective (GP) is the Research and Innovation Policy Stakeholders' Arena, 'policy arena' for short, articulated by Kuhlmann (2001, 2002, and 2003) and Edler and Kuhlmann (2003). As an analytical perspective, the 'policy arena' allows to frame the (interactive) *governance dynamics* of an evolving (social-technical) Science, Technology and Innovation (STI) system or structure. The 'policy arena' characterizes the governance dynamics of a STI system in terms of horizontally and vertically interwoven *multi-tier⁵ logic* (local, regional, national, transnational, international) and *multi-actor logic* (formal and informal networks of competing, cooperating and contesting heterogeneous actors). Figure 10 below depicts the 'policy arena' and its four categories of institutions; these are *the science institutions*, the *industrial institutions*, the *societal institutions*, and the *politico-administrative institutions*.

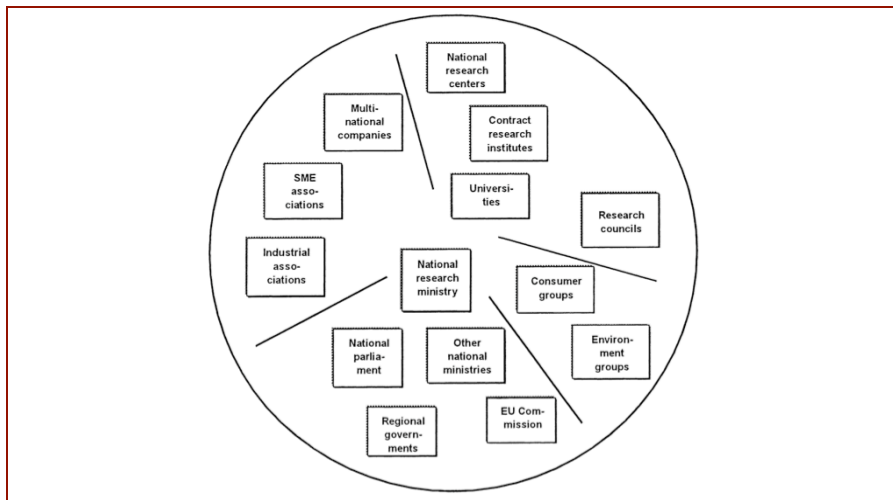


Figure 10 – The Research and Innovation Policy Stakeholders' Arena (Kuhlmann, 2002: 14)

The 'policy arena' as an analytical perspective allows getting insights in the innovation policy processes in arenas that often lack a dominant player or actor. The involved negotiating heterogeneous actors, representing the manifold potentially involved institutions and organizations, play out these innovation policy processes in the arena. These policy processes encompass policy related activities such as option exploration, agenda setting, negotiation, decision-making, implementation, evaluation, interactive and iterative policy learning.

When the 'policy arena' perspective is applied to a given empirical policy context, it allows to identify and structure the involved heterogeneous actors. Consequently, the 'policy arena' also makes apparent the actors that do not participate in the arena, referring those

⁵ In order to prevent confusion with levels of the MLP on socio-technical transition, the 'levels' associated with governance are called 'tiers'.

actors that are excluded from the innovation-policy making negotiations. The actors that do participate in the ‘policy arena’ are subjected to ‘bounded rationality’ as they each bring different perspectives, interests, values, strategies, and power to the negotiation table.

The room of maneuver or leeway the involved actors have is vital for their ability to pursue their autonomous strategic decision-making and action. The actors’ room to maneuver depends on the ‘looseness’ of the arena. For instance, an actor’s ability for autonomous decision-making and successive action is severely restricted when it is locked-in by a coalition, i.e. a constellation of actors.

Overall, within the ‘policy arena’, the participating heterogeneous actors fiercely contest innovation policies. Despite actors’ different perspectives on policy matters, there is a strong emphasis on finding consensus, alignment, and policy learning. The main reasons for this is that the alternative would be ‘no deal’ or even worse, the termination of the negotiations when an actor uses its ‘exit’ option. As all the participating actors know, ‘no deal’ or ‘exit’ would be detrimental to the policy process, as it would only aggravate the dispute and impede upon making progress.

2.3.2 Governance in connected multi-tier and multi-actor policy arenas

Benz (2006) takes the ‘policy arena’ further as he constructs a typology of what he calls ‘governance regimes’. According to Benz (2006: 4), the governance perspective ‘designates a certain analytical perspective determined to make apparently opaque an over-complicated structures and processes of collective action in the state, economy and society comprehensible’ and therefore ‘governance can be made fruitful for the analysis of complex patterns of collective action.’

The typology of governance regimes by Benz (2006), understands governance as a mechanism for control and coordination in complex rule based systems and structures. The structures and systems refer to the heterogeneous independent though connected multi-tier⁶ and multi-actor policy arenas. The connected policy arenas are the dynamic inter-related functional/thematic structures and processes of collective policy-making and action that together make up a complex *governance regime*. Benz (2006) mainly focuses on *regulative* (formal) rules in a governance regime and keeps the *normative* (behavioral) rules and *cognitive* (knowledge) rules in the background. However, Kuhlmann (2007b) commenting on Benz (2006), stresses that the normative rules and the cognitive rules play an important role in the policy-making arenas of a governance regime as well.

According to Benz (2006: 17) ‘in many cases governance regimes emerge in inter-organizational or intergovernmental policy-making between territorial units, levels of governments, states or public and private actors.’ Take for instance societal self-regulation such as cooperative private self-regulation or the cooperation between public actors and private actors. In both cases, the actors pursue to solve collective policy problems with adequate policy-decisions for collective action without the necessary involvement of the political/legislative government.

The typology of governance regimes by Benz (2006) typifies a complex governance regime in terms of governance types or modes of governance; these are *hierarchy*, *network*, *competition*, and *negotiation*. These modes of governance simultaneously characterize the *structures* and *interactions* of the organized actors of a complex governance regime. Consequently, these modes of governance facilitate in describing a complex governance regime and facilitate to understand the specific *mechanisms* and *procedures* that are at work inside it. Often a complex governance regime is best described by a combination of different modes of governance. Consult figure 11 below for an overview of how Benz (2006)

⁶ In order to prevent confusion with levels of the MLP on socio-technical transition, the ‘levels’ associated with governance are called ‘tiers’.

characterizes the structures and interactions among actors in different modes of governance in terms of their relationships, motivation/orientation, and coordination of individual actions. Consult figure 12 below for an overview how Benz (2006) characterizes the structures and interactions of composite governance regimes.

Figure 1: Types of governance

	Hierarchy	Networks	Competition	Negotiation
relationships	asymmetrical permanent	asymmetrical or symmetrical permanent	Symmetrical temporary; issue-specific	Symmetrical temporary; issue-specific
motivation; orientation	egoistic	cooperative	egoistic (comparative advantage)	mixed motives
coordination of individual actions	unilateral adjustment	unilateral and mutual adjustment/trust and consent	mutual adjustment	agreement

Figure 11 – Types or modes of governance (Benz, 2006: 8)

Figure 2: “Composite” governance regimes

	negotiation	competition	network	hierarchy
hierarchy	negotiations in the administrative implementation of laws (“co-operative administration”)	“open method of coordination” benchmarking in regional and local policy	“policy communities” in public administration or between government and private corporations	multilevel hierarchies in public administration
network	administrative networks in the German co-operative federal system	networks among firms; research networks	multi-level networks (networks in networks)	
competition	party competition in the German „co-operative“ federal system	competition among regions in political systems with strong party competition		
negotiation	negotiations in multi-level polities			

Figure 12 – Composite types or modes of governance (Benz, 2006: 9)

Benz (2006) also typifies the policy outcomes (certain and uncertain) of the policy-making processes in an arena and the commitment (strong and weak) the involved actors have to the policy outcomes. See figure 13 below for an overview.

Figure 3: Consequences of rule systems in different governance structures

	hierarchy (agents)	networks	competition	negotiation
outcome of policy-making in an arena	uncertain	certain	certain	uncertain
commitment to policies in an arena	strong	weak	strong	weak

Figure 13 – Policy outcomes in governance regimes (Benz, 2006: 12)

The combination of the ‘policy arena’ and the typology of governance regimes make up the Governance Perspective (GP). The GP is a powerful analytical tool to describe and evaluate the governance dynamics of a complex governance regime. Firstly, the GP enables to identify the policy-making processes in multi-tier and multi-actor connected but functionally independent policy-making arenas that make up a complex governance regime. Secondly, the GP enables to typify the ‘governance dynamics’ of a complex governance regime in terms of modes of governance. Finally, the GP enables to typify the ‘resultants’ of the governance dynamics of the governance regime, i.e. the policy outcomes of the policy-making processes, including the commitment to them by the involved actors.

In this study, the GP will serve to conceptualize the regulatory dimension of socio-technical transition as conceptualized by the MLP. The GP will serve to get insights into the emerging regulative (formal) rules concerning consumer privacy protection of RFID in the European retail sector.

2.3.3 The GP is compatible and complementary with the MLP

In this study, the MLP and the GP together make up the hybrid MLP-GP analytical framework. This framework will function as an analytical perspective to guide the empirical research regarding the regulatory dimension of socio-technical transition. The symbiosis between the MLP and the GP is possible because they are *compatible* and *complementary* with each other.

The MLP and the GP are *compatible* with each other for three reasons. The first reason is that the MLP and the GP both pursue to frame and understand the agency-structure dynamics of co-constructive and co-evolving socio-technical innovative structures or systems. Secondly, both the MLP and the GP provide a causal process oriented model for socio-technical innovation and reason in terms of ‘processes yielding outcomes’. Finally, the MLP and the GP are rule-based models for coordinated action by focusing on the socio-institutional dynamics of a given socio-technical innovative structure or system. Both the MLP and the GP acknowledge regulative (formal), normative (behavioral) and cognitive (knowledge) rules to enable and constrain and thus coordinate (inter)actions among heterogeneous actors. In other words, both the MLP and the GP consider rules and the (inter)actions of actors to be key process variables that affect outcomes.

The MLP and the GP are *supplementary* to each other in the following way. In this study the MLP provides the overarching analytical perspective on socio-technical transition. Because of the broad and multi-faceted nature of the MLP, it does not have any specific analytical perspective to open the ‘black box’ of emerging regulative (formal) rules in the regulatory dimension of socio-technical transition. The GP however, does provide the analytical perspective to do just that. The GP conceptualise the regulatory dimension of the MLP in terms of the governance dynamics of a governance regime. The governance dynamics are the policy processes in connected multi-tier and multi-actor policy-making arenas that yield policy resultants (policy outcomes). Hence, in this study the MLP and the GP are employed in a symbiotic fashion to study the regulatory dimension of socio-technical transition.

2.4 Operationalization of the MLP-GP hybrid analytical framework

Various scholars, of whom Geels and Schot are the most prominent, have constructed the MLP by examining socio-technical patterns of various technological innovations in numerous historical (retrospective) case studies. This study applies the MLP in an experimental fashion to a contemporary real-time case, i.e. a ‘moving target’. In addition, based upon typology of socio-technical transition pathways of Geels & Schot (2007a), this study will make an assessment about the potential near future socio-technical transition pathway, i.e. this study employs the MLP in a ‘prospective fashion’ too.

The operationalisation of the MLP proves to be challenging. The MLP does not provide a systematic way of how an analyst should go about making the translation from the conceptual level to the empirical level, i.e. the case study at hand. In fact, Geels and Schot (2007a) underline that if one wants to apply the MLP, the analyst him/herself has to link the conceptual level to the empirical level. The analyst needs to ‘first demarcate the empirical level of the object of analysis and then operationalise the MLP’ (Geels & Schot, 2007a: 4). In relation to the empirical object of analysis, the analyst thus has to find the relevant organized and situated actors and their relation to the notions of the socio-technical landscape, socio-technical regime, niche innovations, socio-technical regime transition dynamics, and so forth. Genus and Coles (2008) severely criticize Geels and Schot for this major shortcoming, as they call for a serious rethinking of the MLP to improve its operationalisation and hence its systematic development.

As outlined above, this study combines the MLP in a symbiotic fashion with the GP to form the hybrid MLP-GP analytical perspective. The MLP-GP serves for guiding the empirical research for understanding the socio-technical transition dynamics concerning RFID applied on consumer products in the European retail sector. Consumer privacy is the most salient concern of RFID. Consequently, the emerging regulation for consumer privacy protection aims at adequately address these consumer privacy concerns by mitigating the potential negative consequences of RFID for consumer privacy. Adequate regulation for consumer privacy protection therefore plays an important role in the further adoption of RFID in the retail sector in the near future. Following the recipe of Geels and Schot (2007a), the analytical distinctions in this study of the hybrid MLP-GP analytical framework are as follows.

The *incumbent socio-technical regime* that carries and stores the rules of how to use, produce, and regulate the incumbent technology is the *tradition barcode regime*. This regime is characterized by the European Article Number (EAN) and Universal Product Code (UPC) barcodes that are issued by GS1global and are applied on consumer products in the in-store B2C application domain in the retail sector.

The *technological niche* in which experiments in a real-life context are being conducted in a protected environment in order to *learn* how to use, produce, and regulate a radical technological innovation is defined on two levels. On a *global niche-level*, the technological niche is defined as the ‘*emerging field of the EPC standards suite that is issued by GS1global-EPCglobal for the application of RFID on consumer products in the in-store B2C application domain in retail*’, the *RFID technological niche (GS1-EPCglobal-EPC)* for short. On a *local niche-level*, the technological niche is defined by the ‘*RFID pilot projects carried out by the METRO Group Future Store Initiative in local practices in Germany in the EU*’.

The *RFID technological niche* could have the *innovation potential* to provide the conditions for a *socio-technical regime transition* from the *traditional barcode regime* (GS1-EAN/UPC) to the *RFID regime* (GS1-EPCglobal-EPC) within the in-store B2C application domain in the retail sector. To investigate to what extent these conditions are satisfied, the ‘black box’ of the regulatory dimension of socio-technical transition needs to be opened.

The GP will serve to do this by laying bare the *governance dynamics* of the *emerging governance regime* for *consumer privacy protection*. In doing so, the GP enables to get insights into the *policy outcomes for collective action* concerning consumer privacy protection that are the ‘resultants’ of the *policy processes of collective decision-making*. These policy processes refer to the socio-institutional dynamics of the cooperating, competing, and contesting heterogeneous private and public stakeholders concerning the emerging predominantly regulative (formal) rules. These socio-institutional dynamics are played out in connected multi-tier and multi-actor policy-making arenas. This study therefore aims to identify possible local, regional, national, transnational, and international connected policy-making arenas. This includes the actors from the categories of institutions (industrial, societal, science, politico-administrative) such as retail, industry, consumer, privacy, and governmental organizations inside them that together make up the emerging governance regime for consumer privacy protection. In addition, this study aims to characterize the structure and interactions of the actors in the identified policy-making arenas in terms of the modes of governance. This study also aims to interpret the regulatory outcomes in the identified policy-making arenas.

The insights into the *governance dynamics* of the *emerging governance regime* for *consumer privacy protection* are subsequently interpreted by the typology of five socio-technical transition pathways by Geels and Schot (2007a). This will enable to speculate upon the most plausible near future *socio-technical transition pathway* for the potential regime transition from the *traditional barcode regime* to the *RFID regime* in European retail sector in the near future.

The socio-technical transition dynamics take place against the backdrop of the *socio-technical landscape* that is defined as the technical, physical, and material backdrop that sustains the contemporary global information society. In the current information society, the *high-speed transportation technologies* (e.g. rail, road and air travel) work in tandem with the *high-speed information and communication technologies* (ICTs) (e.g. telephone, radio, television, and the Internet). In addition, in the information or knowledge society, digital information is increasingly considered the most important commodity (Scheuermann, 2006; Castells, 1996; Stalder, 1998).

2.5 Conceptual-laden research questions

Based upon the previous discussion about the hybrid MLP-GP analytical framework and its operationalization, we are now able to reformulate the empirical research questions as stated in the introduction. The following are the conceptual-laden research questions.

Question 1 (Q1): ‘What is the socio-technical configuration of the RFID pilot projects undertaken by the METRO Group Future Store Initiative (MGFSI) in the RFID technological niche?’

Question 2 (Q2): ‘What are the interest groups, main actors, and their perspectives in the emerging governance regime for consumer privacy protection?’

Question 3 (Q3): ‘What do the main actors in the emerging governance regime for consumer privacy protection perceive to be the external socio-technical landscape pressures on the traditional barcode regime and on the RFID pilot projects undertaken by the MGFSI in the RFID technological niche?’

Question 4 (Q4): ‘How can we understand the resultants (policy outcomes) of RFID-specific consumer privacy regulation in terms of the governance dynamics (multi-tier and multi-actor policy processes) of the emerging governance regime for consumer privacy protection?’

Question 5 (Q5): ‘How do **Q1-Q4** contribute to a discussion on an outlook whether there will be ‘multi-level alignment’ and a ‘window of opportunity’ for the RFID technological niche to have the innovation potential to provide the conditions for a socio-technical regime transition, via a specific transition pathway, from the traditional barcode regime to the RFID regime in the near future?’

Question 6 (Q6): ‘How do **Q1-Q5** contribute to formulating a policy recommendation concerning the adoption of RFID in the European retail sector?’

Question 7 (Q7): ‘How do **Q1-Q5** contribute to formulating a conceptual contribution to the hybrid MLP-GP analytical framework?’

3. Research methodology and strategy

3.1 An RFID governance case study

This study conducted a RFID governance case study to get in-depth and state-of-the-art insights into the embryonic, innovative, and dynamic empirical research field of emerging regulation for consumer privacy protection of RFID. This as RFID is applied on consumer products (CPILT) in the front-end and in-store business-to-consumer (B2C) application domain in the European retail sector. This chapter presents the empirical methodology and research strategy of how the RFID governance case study by applying the hybrid MLP-GP analytical framework as discussed in the previous chapter was conducted. This chapter therefore will indicate how the RFID governance case study established the symbiotic relationship between the conceptual level and the empirical level, as it integrated conceptual notions with empirical data from the research field (Eisenhardt, 1989; Eisenhardt & Graebner, 2007).

By conducting a RFID governance case study, this study aimed to lay bare the *governance dynamics* of the *emerging governance regime* for *consumer privacy protection* in the European retail sector. This implied identifying the multi-tier (local, regional, national, transnational, international) connected policy-making arenas; see figure 14 below. These policy arenas are inhabited by heterogeneous organizations from the institutional clusters (industrial, societal, politico-administrative, and science) such as retail, industry, privacy, consumer, and governmental organizations (multi-actor).

In this chapter, section 3.2 will present the criteria that were used when executing the RFID governance case study. Section 3.3 will present the identified tiers, the identified involved organizations, and the methods that were used to acquire the necessary primary empirical data from them. Finally, section 3.4 will describe how the data from the empirical research field was incorporated into the RFID governance case study.

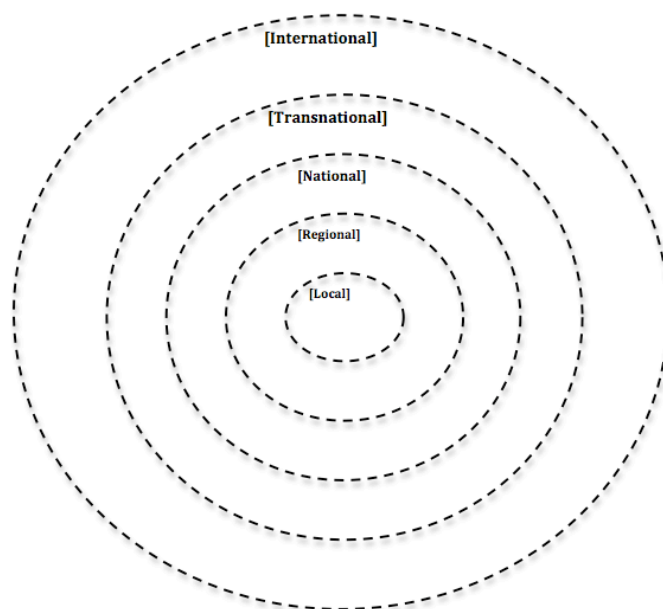


Figure 14 - The multi-tier and multi-actor emerging governance regime for consumer privacy protection

3.2 Criteria for the execution of the RFID governance case study

In the execution of the RFID governance case study, the following criteria for identifying the organizations conducting the RFID pilot projects and the other involved organizations in emerging governance regime were taken into account. The *first criterion* was that the RFID pilot projects were undertaken by a retailer that experimented with the application of RFID on consumer products (CPILT) in the front-end and in-store B2C application domain in the retail sector. In other words, RFID pilot projects that are conducted under real-life conditions in the public sphere, as opposed to being isolated in a test or research lab behind closed doors. The *second criterion* was that due to the practical structure of this study, the RFID pilot projects and the other involved organizations in the emerging governance regime had to be located in the EU and or in the US. The *third criterion* was that the retailer that was conducting the RFID pilot projects participated in an emerging governance regime for which there were strong indications that there were interesting governance dynamics going on. The *fourth criterion* was that the retailer conducting the RFID pilot projects and the other involved organizations in the emerging governance regime needed to be accessible in order to get the necessary empirical data of the governance dynamics for the RFID governance case study.

3.3 Scope and execution of the RFID governance case study

3.3.1 Initial research field screening

The RFID pilot projects undertaken by the METRO Group Future Store Initiative (MGFSI) located in Germany and the other involved organizations in the emerging governance regime satisfied the four criteria as stated in the previous section. They were publicly accessible, located in the EU, and were showing promising governance dynamics.

The articles, documents, and web pages examined for the first part of the RFID governance case study, as presented in chapter 4, functioned as the starting point in conducting the *initial research field screening*. The initial research field screening enabled me to identify the tiers and the key involved organizations of the emerging governance regime. This led me to construct the visual chart of the emerging governance regime centered on the RFID pilot projects of the MGFSI. Respectively, I identified the local, regional, national, transnational, and international tier by the RFID pilot projects of the MGFSI, Nordrhein-Westfalen (NRW), Germany, European Union, and EU-US Transatlantic. In addition, the initial research field screening led me to develop the *initial open-ended interview questions* for the semi-structured qualitative interviews with several of the identified key organizations in the emerging governance regime.

The next sections present the tiers and the organizations I identified for the emerging governance regime. The sections also describe the methods for their empirical study, as they participated in the RFID governance case study.

3.3.2 Local tier of the emerging governance regime

To get insights into the local tier of the emerging governance regime for consumer privacy protection, I visited the RFID pilot projects undertaken by MGFSI, including the European EPC Competence Center that is co-housed with the METRO Group RFID Innovation Center. All these organizations are located around Düsseldorf in Nordrhein-Westfalen (NRW), the biggest federal state of Germany in economical terms. Table 2 below presents the experts of the organizations who participated in the RFID governance case study by means of an *interactive guided tour session*.

Organization	Category of institution	Location	Name tour guide	Function	Date visited
METRO Group REAL Future Store (Supermarket)	Industrial	Toenisvorst, Germany	Jan Lingenbrinck	Communications and Public Affairs	02-07-2008
METRO Group RFID Innovation Centre	Industrial	Neuss, Germany	Laura Mueller	Communications and Public Affairs	04-07-2008
European EPC Competence Centre (EECC)	Industrial	Neuss, Germany	Thomas Holtstiege	Senior Test Engineer	04-07-2008
METRO Group Galeria Kaufhof (Department Store)	Industrial	Essen, Germany	Martin Haeussler	Project RFID Merchandise-Management and Information systems	07-07-2008

Table 2 - Organizations on the local tier of the emerging governance regime

To identify these organizations of the emerging governance regime, the website of the MGFSI provided to be a useful source as it contained elaborate information about their RFID pilot projects and related RFID activities. In a nutshell, the MGFSI is famously known for its initial attempts to experiment with the RFID technology on consumer products in the REAL Future Store in Rheinberg in Germany, already dating back to 2003. This is the initial RFID pilot project in the real-life context that caused the major consumer privacy controversy concerning the customer loyalty cards. In 2004, the MGFSI opened the RFID Innovation Center. This is a RFID test and research lab that functions next to an information and exhibition lab as a RFID development platform. Since August 2007 the MGFSI has launched a RFID pilot project in the department store Galeria Kaufhof, located in Essen Germany. Here they experiment with the application of the RFID technology on menswear in the department store setting. In May 2008, the MGFSI has opened the renewed REAL Future Store located in Toenisvorst Germany. Here the MGFSI applies RFID on meat packaging in the intelligent fridge, as one of the innovative ambient technologies they are experimenting with in the supermarket setting.

To get a real-life-look-and-feel experience of the RFID pilot projects, I scheduled an *interactive guided tour session* with these organizations. During the guided tours, I was able to observe and simultaneously ask questions concerning their RFID activities. In the case of the REAL Future Store in Toenisvorst, this was combined with the *semi-structured interview session*. For this session, I drew upon the prepared guiding open-ended interview questions in order to gain deeper understanding of their RFID activities. For the other organizations, the guiding open-ended interview questions were in the back of my mind as I prepared thoroughly for the guided tour. This as I was unable to record the sessions, due to the practical impossibility as I was shown around the compound, or after being declined after requesting it. In these cases, immediately after the guided tour session, I crystallized my empirical findings in my *field notes*. After each guided tour, I updated the chart of the emerging governance regime and the open-ended interview questions; these I was also to employ during the semi-structured interviews on the regional and national tier of the emerging governance regime.

After the *interactive guided tour sessions*, there were still several missing bits and pieces to complete the RFID governance case study. Hence, I sent out an email questionnaire with specific questions to the organizations that potentially had the missing information concerning the local tier of the emerging governance regime. Table 3 below presents an overview of the organizations and persons with whom I had email correspondence accordingly.

Organization	Category of institution	Location	Name Correspondent	Function/Division
METRO Group Information Technology (MGI)	Industrial	Dusseldorf, Germany	Daniel Kitscha	Communications & Public Affairs
Auto-ID labs University of St. Gallen	Science	St. Gallen, Switzerland	Dr. Frederic Thiesse	Associate Director Auto-ID Labs / Project Manager M-Lab

Table 3 - Email correspondence concerning the local tier of the emerging governance regime

3.3.3 Regional tier and national tier of the emerging governance regime

To get insights into the regional tier and national tier of the emerging governance regime for consumer privacy protection, I visited an organization in Nordrhein-Westfalen (NRW) and organizations located around Germany's political capital Berlin. Table 4 presents the experts in the organizations who participated in the RFID governance case study by means of a *semi-structured interview session*.

Organization	Category of institution	Location	Name Interviewee	Function	Date visited
Consumer Center Nordrhein-Westfalen (VZ-NRW)	Societal	Düsseldorf, Germany	Dipl. Kauffrau Brigitte Rittmann-Bauer	Consumer Counseling (Consumer interest and retail)	07-07-2008
Association for the Promotion of Public Mobile and Immobile Data (FoeBuD)	Societal	Bielefeld, Germany	Rena Tangens	Co-founder FoeBuD	21-07-2008
Informationsforum RFID	Industrial	Berlin, Germany	Simon Japs	Government Affairs Manager	22-07-2008
Berlin Commissioner for Data Protection and Freedom of Information	Politico-administrative / Societal	Berlin, Germany	Dr. Alexander Dix	Berlin Commissioner for Data Protection and Freedom of Information	23-07-2008
Federation of German Consumer Organizations (Federal Consumer Center) (VZ-BV)	Societal	Berlin, Germany	Katja Mrowka and Dr. Christian Thorun	Policy Officer Commercial Law, Trade and Competition, Policy Officer trade and Economic Policy	24-07-2008
Nature and Biodiversity Conservations Union (NABU)	Societal	Berlin, Germany	Dr. Benjamin Bongardt	Head of Environmental Politics	25-07-2008

Table 4 - Organizations on the regional tier and national tier of the emerging governance regime

To identify these organizations of the emerging governance regime, I employed a four-step strategy. *Step one*, was to send an email invitation letter to the organizations that came up during the *initial research field screening*. The email invitation letter covered the research theme, research purpose and what was required from the organizations to participate in the research. In order to mitigate informant bias and to get a balanced in-depth understanding of the governance dynamics of the emerging governance regime the RFID governance case study needed the perspectives of different organizations. Therefore, a balanced set of heterogeneous organizations was approached to participate in the research. *Step 2* was to follow up after the sent email invitation letters by phoning the approached organizations. This made sure that the email invitation letters reached the right expert within the organizations or it enabled direct contact with the experts. *Step 3* was to schedule the real-life face-to-face semi-structured interview with the experts of the organizations that wanted and could participate in the research. Some organizations declined, due to a lack of resources or because they could not participate in the research as they did not have an expert on the subject matter. In these cases, they recommended alternative comparable organizations that had a similar perspective and interest in the subject matter of the case study. *Step 4* was to prepare the experts within the organization for the scheduled semi-structured interview. To that end, the chart of the emerging governance regime and the open-ended interview questions for the semi-structured interviews were sent to them in advance by email.

During the *semi-structured interview session*, the physical chart of the emerging governance regime that captures the organizations involved in the governance dynamics proved to be a valuable tool in getting the interview started and more importantly going. The accompanied semi-structured interview drawing upon the guiding open-ended interview questions functioned as a metaphorical 'fishnet'. It enabled to get salient state-of-the-art and in-depth information that I did not expected to acquire upfront. Consequently, I was able to

dig deeper into interesting points that surfaced during the interview. Upon executing the interview, the guiding open-ended interview questions functioned as a backup in case required. This allowed me to develop the semi-structured interview regarding the governance dynamics of the emerging governance regime as natural and spontaneous as possible. This was also supported by the fact that I was allowed to record the semi-structured interviews. Please consult the next two chapters for the emerging governance regime charts. The associated guiding open-ended interview questions are enclosed in Appendix A.

After the *semi-structured interview sessions*, there were still several missing bits and pieces to complete the RFID governance case study. Hence, I sent out an email questionnaire with specific questions to the organizations that potentially had the missing information concerning the regional and national tier of the emerging governance regime. Table 5 below presents an overview of the organizations and persons with whom I had email correspondence accordingly.

Organization	Category of institution	Location	Name Correspondent	Function/Division
Informationsforum RFID	Industrial	Berlin, Germany	Simon Japs	Government Affairs Manager
Federation of German Consumer Organizations (VZ-BV)	Societal	Berlin, Germany	Christian Thorun	Officer trade and Economic Policy
Berlin Commissioner for Data Protection and Freedom of Information	Politico-administrative / Societal	Berlin, Germany	Axel Toenjjes	Berlin Commissioner for Data Protection and Freedom of Information
GS1-Germany	Industrial	Koln, Germany	Sandra Hohenecker	Senior Product Manager
Federal Commissioner for Data Protection and Freedom of Information (BfDI)	Politico-administrative / Societal	Bonn, Germany	Dirk Bungard	Federal Commissioner for Data Protection and Freedom of Information

Table 5 - Email correspondence concerning the regional and national tier of the emerging governance regime

3.3.4 Transnational and international tier of the emerging governance regime

To get insights into the transnational and international tier of the emerging governance regime for consumer privacy protection, I attended a public policy oriented symposium and workshop, and a business and technology oriented conference. These were organized in the EU-US transatlantic context. In addition to the semi-structured interviews with key organizations, this further illuminated my insights of the research field by approaching and understanding it from different angles. The attendance updated my knowledge of the governance regime as I had the ability to listen, observe, and talk to experts who represented key heterogeneous organizations that take part in the emerging governance regime.

The symposium I attended was the ‘Transatlantic Symposium on the Societal Benefits of RFID’ in Washington D.C. on 22 September 2008.⁷ This symposium was co-hosted by the TransAtlantic Business Dialogue (TABD)⁸, European-American Business Council (EABC)⁹, and EPCglobal¹⁰, with the support of the US Department of Commerce¹¹ and the Information Society and Media Directorate-General of the European Commission (DG INFSO).¹² The main objective of this symposium was to encourage a dialog between business, consumer, and governmental organizations ‘on the rapidly developing technology of radio frequency

⁷ For more information about this event consult: http://www.tabd.com/index.php?option=com_content&task=view&id=89&Itemid=99.

⁸ For more information about the TransAtlantic Business Dialogue (TABD) consult: <http://www.tabd.com/>.

⁹ For more information about the European-American Business Council (EABC) consult: <http://www.eabc.org/>.

¹⁰ For more information about EPCglobal consult: <http://www.epcglobalinc.org/>.

¹¹ For more information about the U.S. Department of Commerce consult: <http://www.commerce.gov/>.

¹² For more information about the Information Society and Media Directorate-General of the European Commission (DG INFSO) consult: http://ec.europa.eu/dgs/information_society/.

identification (RFID) in order to support and advance the Lighthouse Project on Innovation and Technology from the 2007 US-EU Summit declaration' (TABD, 2008). Particularly interesting for this study was the fourth panel discussion entitled 'Future Applications of RFID to Enhance End-to-End Consumer Experience in retail' (TABD, 2008). During this panel discussion, the METRO Group gave a case presentation of their activities and experiences with RFID applied on consumer products in their RFID pilot projects of their Future Store Initiative.

The symposium was jointly organized with the 'Transatlantic RFID Workshop on Consumer Privacy and Data Security' in Washington D.C. on 23 September 2008.¹³ This workshop was co-hosted by the Federal Trade Commission (FTC)¹⁴ and Information Society and Media Directorate-General of the European Commission (DG INFSO). The purpose of this workshop was to explore the 'emerging applications of radio frequency identification (RFID) technology and their implications for consumer protection policy' (FTC, 2008c). The workshop brought together representatives from the industry, government officials, and consumer advocates from the EU and the US to discuss privacy and security concerns associated with RFID. In addition, during the workshop the participants explored possible solutions and consumer awareness and education initiatives regarding these concerns. Particularly interesting for this study was the panel discussion on emerging utilization of the item-level tagging in the retail sector. During this discussion Wal-Mart Inc.¹⁵ gave a presentation on their past experiences and future expectations concerning the application of RFID on consumer products, as they currently do not have any RFID pilot projects.

The conference I attended was the 'EPCglobal Connection 2008 -- Fifth Annual Conference and Exhibition' co-hosted by RFID Journal¹⁶ and EPCglobal on 14-16 October in Chicago.¹⁷ With the conference, EPCglobal as the subdivision of GS1global¹⁸ wants to promote the Electronic Product Code (EPC) standards suite as the global standard for the RFID technology in a variety of industries. EPC is the successor of the GS1global's barcode also known as the European Article Number (EAN) in Europe and the Universal Product Code (UPC) in the US. Key industries for which RFID has great potential benefit are the retail industry, the pharmaceutical industry, the defense industry, the identification/security industry, the public transportation industry, and the financial industry. During the conference, I had the ability to attend the conference sessions and talk to a variety of companies as they had an exhibition stand in the exhibition hall. Furthermore, I had the opportunity to chair the 'Supply Chain' track as one of the four parallel tracks in the conference. The other tracks were 'Manufacturing', 'EPC in the Defense industry', and 'Retail Supplier Implementation'. This conference made clear that the application of RFID on consumer products in the B2C domain is still far away. The current focus is on stimulating the application of RFID in the B2B supply chain, i.e. on pallets, crates, and boxes.

The 'EPCglobal Connection 2008', was private sector oriented, as it focused on the business and technological aspects of the RFID technology in a variety of industrial application domains. The 'Transatlantic Symposium on the Societal Benefits of RFID' and 'Transatlantic RFID Workshop on Consumer Privacy and Data Security' were public sector oriented, as they focused on the public policy issues associated with the RFID technology. Because of their complementary nature, the symposium, workshop, and conference provided an overall (private-public), state-of-the-art, and in-depth perspective on RFID and its

¹³ For more information about this event consult: <http://www.ftc.gov/bcp/workshops/transatlantic/index.shtml>.

¹⁴ For more information about the Federal Trade Commission (FTC) consult: <http://www.ftc.gov/>.

¹⁵ For more information about Wal-Mart Inc. consult: <http://walmartstores.com/>.

¹⁶ For more information about RFID Journal consult: <http://www.rfidjournal.com/>.

¹⁷ For more information about this event consult: <http://www.epcconnection.com/>.

¹⁸ For more information about GS1global consult: <http://www.gs1.org/>.

consumer privacy concerns. Hence, the attendance of the events in Washington D.C. and in Chicago made a valuable contribution to the RFID governance case study.

After the *symposium, workshop, and conference attendance*, there were still several missing bits and pieces to complete the RFID governance case study. Hence, I sent out an email questionnaire to the organizations that potentially had the missing information concerning the transnational and international tier of the emerging governance regime. Table 6 below presents an overview of the organizations and persons with whom I had email correspondence accordingly.

Organization	Category of institution	Location	Name Correspondent	Function/Division
European Commission: DG Information Society and Media (DG INFSO)	Politico-administrative	Brussels, Belgium	Manuel Mateo Goyet	Scientific and Policy Officer (D4 - Networked Enterprise & Radio Frequency Identification)
Federal Trade Commission (FTC)	Politico-administrative	Washington D.C., United States	Kathryn Ratté	Division of Privacy and Identity Protection
EPCglobal	Industrial	Washington D.C., United States	Elizabeth Board	Executive Director of the EPCglobal Public Policy Steering Committee
Organization for Economic Co-operation and Development (OECD)	Politico-administrative	Paris, France	Laurent Bernat and Karine Perset	Information, Computer and Communications Policy Division of the Directorate for Science, Technology and Industry

Table 6 - Email correspondence concerning the transnational and international tier of the emerging governance regime

3.4 Analysis and reporting

For the analysis and presenting the description of the RFID governance case study, I drew upon the empirical data gathered during the interactive guided tours, the semi-structured interviews, the RFID symposium, workshop and conference attendance, and email correspondences of the research field. The empirical data consists of the empirical observations I made during the interactive guided tours, my field notes, audio recordings of the interviews, the documents that were handed over to me during or after the interviews, the documents retrieved from the organizations' websites, personal notes, presentations and brochures from the RFID symposium, workshop and conference, and emails. The primary empirical data was *supplemented* by document study of privacy policy related documents that I retrieved from websites of (privacy) policy organizations. In addition, I studied secondary literature from scientific journals and books concerning consumer privacy and RFID applied on consumer products.

During the overall execution of this study, I employed a digital file database on my computer for storing, sorting, and retrieving all the gathered heterogeneous primary and secondary data sources in a systematic and comprehensive way. Data sources included in the digital database are the articles, brochures, research reports, policy documents, policy reports, web pages and their bookmarks, email correspondences, recorded interviews, field notes, scanned actor documents, pictures, documentaries, and short movies. Consequently, the extensive database of digital files facilitated in the *triangulation* process that had the aim of *corroborating* the research findings and conclusions following the analysis of the RFID governance case study.

The results of the RFID governance case study are presented in the next two chapters, answering conceptual-laden research questions Q1-Q4. Chapter 4 will present the first part of the RFID governance case study. This chapter investigates the need for a RFID-specific regulatory capability for consumer privacy protection in the European retail sector. Chapter 5 subsequently will present the second part of the RFID governance case study. This chapter investigates the emerging RFID-specific regulatory capability for consumer privacy protection in the European retail sector. Subsequently chapter 6, by answering conceptual-laden research questions Q4-Q7, will reflect upon the RFID governance case study in the light of the hybrid MLP-GP analytical framework as discussed in chapter 2.

4. RFID governance case study part one – The need for a RFID-specific regulatory capability for consumer privacy protection in retail

4.1 Introduction

This chapter covers the *first part* of the RFID governance case study of the EU and answers conceptual-laden research questions Q1-Q4. The analysis is centered on the METRO Group Future Store Initiative (MGFSI). Since 2003, the MGFSI has been conducting RFID pilot projects on Consumer Product Item-level Tagging (CPILT) in the front-end and in-store Business-to-Consumer (B2C) application domain in the retail sector. This chapter presents the key events regarding the development and application of RFID on consumer products between 2002 and 2005 that triggered the need for a RFID-specific regulatory capability for consumer privacy protection of RFID in the European retail sector. This chapter therefore paves the way for the description and analysis of the emerging governance regime for consumer privacy protection of RFID in the next chapter, part two of the RFID governance case study.

In the following, section 4.2 explains how the Electronic Product Code (EPC) as a global standard for RFID on consumer products came into being and is promoted by the EPC network, led by EPCglobal. Section 4.3 continues by showing that the consumer privacy controversies of EPC applied on consumer products were triggered by consumer privacy NGOs. Section 4.4 then shows how the METRO Group as one of the first retailers in Europe pioneered the EPC technology in a real-life RFID pilot project. As with a lot of pioneering activities, things go wrong and lessons need to be learned. The analysis therefore covers what the METRO Group did wrong concerning consumer privacy in their initial RFID pilot project, again triggered by consumer privacy NGOs. Finally, section 4.5 presents the regulatory response of the global EPC industry to the consumer privacy issues associated with the application of EPC on consumer products in the retail sector.

4.2 The global Electronic Product Code (EPC) standards suite¹⁹ (Q1+Q2)

4.2.1 The birth of EPCglobal

The application of RFID in the retail supply chain has its roots in the Distributed Intelligence Systems Center (DISC) of the Massachusetts Institute of Technology (MIT) in the United States (US) (Sarma, 2005; RFID Journal, 2009). The successor of DISC, the Auto-Identification (ID) Center, or Auto-ID Center for short was launched in September 1999. The Auto-ID Center was co-founded with the former Uniform Code Council (UCC) that administered the Universal Product Code (UPC) barcode, Proctor & Gamble (P&G)²⁰, and Gillette.²¹ Together with more than 100 partners from industry and academia, the Auto-ID Center aimed at developing low cost hardware, software, networks, protocols, standards, and other components of RFID systems. In other words, the Auto-ID Center's main goals were to device the basic architecture for the Internet of Things (IoT). Between its foundation in 1999 and 31 October 2003 due to its success, the Auto-ID Center made a transition to a global research network consisting out of seven Auto-ID laboratories. An additional of six Auto-ID Labs were founded connected to academic institutions. These Auto-ID labs²² are located at St. Gallen & ETH Zurich in Switzerland, Daejeon in Republic of Korea, Keio in Japan, Cambridge in UK, Fedan in China, and Adelaide in Australia (Auto-ID, 2009). By developing a global and multi-industry RFID standard, the network of Auto-ID Labs aims at harmonizing the regional technological differences of Europe, America, and Asia.

In September 2003, EPCglobal as the commercial though not-for-profit spin-off organization from the Auto-ID labs was founded in joint venture with the Uniform Code Council (UCC) and EAN International (EPCglobal, 2009d). Since the 1980s, UCC administered the UPC barcode in the US and EAN International administered the European Article Number (EAN) barcode in Europe. In February 2005, UUC and EAN merged into GS1 global, making EPCglobal a subsidiary of GS1 global.²³ EPCglobal is responsible for the management and promotion of the EPCglobal network and the EPC RFID standards, protocols and interfaces. The network of Auto-ID labs on the other hand is responsible for the foundational Research & Development (R&D) of the RFID technology. Concretely, EPCglobal, having agencies on national levels, manages and promotes the Electronic Product Code (EPC) and the EPCglobal network, the 'EPCglobal standards suite' for short. EPCglobal promotes the EPCglobal standards suite as the global and multi-industry successor of GS1's EAN and UPC barcodes, the current standard in the retail industry. EPCglobal's multi-industry and global ambitions become apparent by the composition of the members of EPCglobal's board of governance (EPCglobal, 2009a). Zygmunt Mierdorf, a member of the management board of the METRO Group, represents the METRO Group in EPCglobal's board of governance.

¹⁹ Unless indicated otherwise this section is based upon: EPCglobal, 2009d, and my conference attendance of EPC Connection 2008 on 14-16 October 2008 in Chicago.

²⁰ For more information about Proctor and Gamble consult: <http://www.pg.com/>.

²¹ For more information about Gillette consult: <http://www.gillette.com/>.

²² For more information about the Auto-ID labs consult: <http://www.autoidlabs.org/>.

²³ For more information about GS1global consult: <http://www.gs1.org/>.

4.2.2 EPCglobal promotes the EPC as the successor of the EAN and UPC barcodes

4.2.2.1 The basics of the EPC

The EPCglobal standards suite is as an extension or add-on to the existing GS1's EAN and UPC barcodes. The barcode on a consumer product carries information about the manufacturer and additional information relevant for the retail supply chain. The barcode enables to identify a group of the same consumer products: 'barcode = company prefix + article number'. For instance, each pair of a particular type of sunglasses from the same brand carries the same barcode, identifying the product group in the retail supply chain. The EPC extends the barcode with an additional number creating a global unique identification number on a par with a license plate: 'EPC = barcode (company prefix + article number) + serial number'. EPC therefore is backwards compatible with the barcode. The EPC as a unique global identification number is stored on the RFID tag that is attached to the item or object in the retail supply chain. The EPC therefore enables the unique identification of consumer products in the retail supply chain, a process that is called 'serialization'. Going back to the example, each pair of a particular kind of sunglasses from the same brand with an EPC carries a different unique identification number, making each of them uniquely identifiable within the product group in the retail supply chain.

The EPCglobal network, the information and database network service of EPCglobal, enables the sharing of supply chain information amongst EPC business and trading partners. By means of the EPCglobal network, consumer products to which an RFID tag is attached that stores an EPC number becomes uniquely identifiable in the global EPC enabled retail supply chain. To illustrate, the EPCglobal network works on top of the Internet. The Internet has a Domain Name Server (DNS) that enables the unique identification of web addresses on a global level. Similarly, the Object Name Service (ONS), the key component of the EPCglobal network, enables the unique identification of an EPC number that is stored on the RFID tag that is attached to an object. The Object Name Server, or the EPC root server, is just as several DNS servers of the Internet managed by VeriSign²⁴, a well-known trusted third party of Internet infrastructure services. See figure 15 below for a simplified graphical representation of an EPC RFID tagged pair of sunglasses that is uniquely identifiable on global level by means of the Object Name Service of EPCglobal.

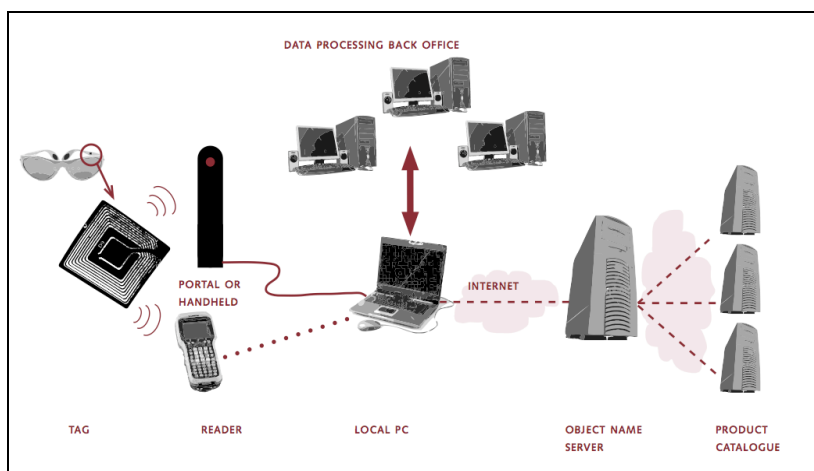


Figure 15 - The Object Name Service (ONS) (Beugelsdijk, 2006: 18)

²⁴ For more information about VeriSign consult: <http://www.verisign.com/>.

4.2.2.2 EPC in the retail value chain

The promise of the EPCglobal standards suite as articulated by the EPC network is that it enables to digitally and real-time identify, track and trace items or objects in the retail supply chain. In contrast to the barcode on items that are scanned with optical (laser) barcode scanners, RFID does not have to be in the line-of-sight. Another advantage is that RFID tags can be read in bulk, for instance a pallet stacked with RFID tagged items can be read in the blink of an eye. EPC therefore allows for the automation, streamlining, and integration of the retail value chain. See figure 16 below for a simplified version of the retail value chain. The retail value chain stretches from manufacturer through intermediate parties and distribution centers to retailers and potentially beyond the point of sale. EPC has the potential to do away with unnecessary human intervention and potential human error, as objects such as pallets, crates, and eventually consumer products traverse through the automated EPC enabled retail supply chain.

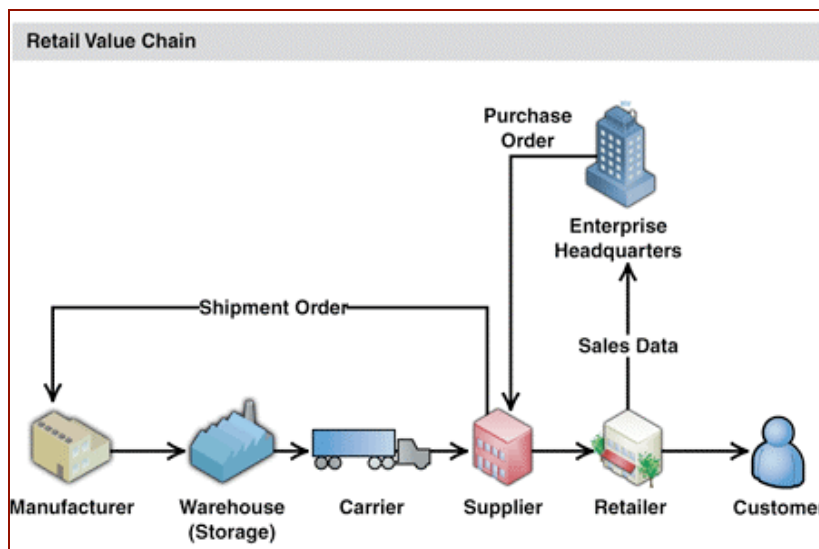


Figure 16 – The Retail Value Chain (MSDN, 2006)

The promise of the EPC standards suite holds that real-time supply chain management enables to closely couple supply and demand. Its chief aim is to reduce out of stocks at the retailers in order to keep the shelves replenished with consumer products. Out of stocks or empty shelves is the number one fear of retailers, as they are unable to sell their products. In addition, out of stock is the number one source of frustration for customers, as they need to go elsewhere to purchase their products. The EPCglobal standards suite also aids in warranting product authenticity (anti-counterfeiting) and functions as anti-theft prevention as the whole retail supply chain is digitally monitored from manufacturer to the point of sale at the retailer. At the point of sale, RFID readers could enable auto checkout at the retailer, reducing waiting lines, as people do not have to place the items of the belt to be scanned by the cashier. Even beyond the point of sale, RFID tagged consumer products may have potential post-purchase benefits such as in intelligent refrigerators, intelligent washing machines and intelligent wine cabinets. By employing the EPC standards suite for the management of the retail supply chain, unprecedented (time) efficiency and visibility or transparency of the retail supply chain is possible. According to EPC network, these gains translate to economical gains for participants in the retail value chain including consumers.

For businesses the investments in the EPC RFID infrastructure is the main issue, i.e. the return on investment. In order for EPC to be profitable on items in the supply chain as with barcodes today, EPC needs to be applied by the manufacturer of the product, so-called 'source-tagging'. In addition, once every party in the supply chain has installed the EPC

infrastructure, they all can benefit from the technology, similar to barcodes today. The cost of the EPC infrastructure investment and the return on investment is a ‘chicken-egg problem’. The demands for EPC technology need to rise that only happens as cost for the investments drop that only happens when demand rises as a result of economies of scale and so forth. This problem makes the adoption of the EPC standards suite in the retail supply chain a slow process.

4.2.2.3 Interoperability by means of the EPC Gen. 2 standard

At the heart of the EPC RFID standard suite that is employed for the management of the retail supply chain and retail inventory management today is the ‘RFID air interface’. The RFID air interface allows RFID transponders/tags and RFID interrogators/readers from different manufacturers and in different parts of the world to talk to each other (interoperability). The official name of the RFID air interface is ‘EPC Radio-Frequency Identity Protocols Class-1 Generation-2 Ultra High Frequency (UHF) RFID Protocol for Communications at 860 MHz – 960 MHz, version 1.2.0 of 23 October 2008’ (EPCglobal, 2009b). This RFID air interface also goes by the ‘ISO 18000-6 part C standard’. The communication between the RFID tag and RFID reader or interrogator via the EPC Gen. 2 air interface standard takes place by means of a process that is called ‘backscatter’ (mirror). This means that the antenna of the passive RFID tag captures the electromagnetic energy emitted by the reader. The energy powers the microchip on the RFID tag and the EPC information is send back to the reader via the antenna of the RFID tag.

The EPCglobal standards suite provides interoperability between RFID components and systems the world over. For instance, the EPC RFID standard accommodates radio frequency spectrum differences between the Europe, America, and Asia. The main organizations that are managing these radio frequencies are the European Telecommunications Standards Institute (ETSI)²⁵ (EU), the Federal Communications Commission (FCC)²⁶ (US), and the International Telecommunication Union (ITU)²⁷ (Global). Consequently, EPCglobal stays into close contact with these organizations as their decisions directly affect the EPC standards suite.

4.2.2.4 The EECC and RFID Journal assist EPCglobal in the promotion of the EPC

The European EPC Competence Center (EECC)²⁸ in Neuss located in Germany is the major test facility for EPC RFID components such as tags, readers, protocols, etc. in Europe (EECC, 2009). EPCglobal certified the EECC as the first ‘European EPCglobal Performance Test Center’ in September 2005. The EECC is a joint venture of GS1 Germany²⁹, Deutsche Post World Net (DHL)³⁰, Karstadt Warenhaus³¹ and the METRO Group.³² The EECC as an RFID testing laboratory aims at fostering the adoption of the global and multi-sector EPCglobal standards suite in Europe. Besides testing, the EECC also offers independent in-house studies of benchmarking RFID components and it offers training and courses for companies that want to start with EPC in their business processes. As EPCglobal and the EECC concern themselves with establishing RFID standards, they work together with International Standardization Organizations (ISO).³³ Moreover, EECC works together with RFID journal³⁴

²⁵ For more information about the European Telecommunications Standards Institute (ETSI) consult: <http://www.etsi.org/>.

²⁶ For more information about the Federal Communications Commission (FCC) consult: <http://www.fcc.gov/>.

²⁷ For more information about the International Telecommunication Union (ITU) consult: <http://www.itu.int/>.

²⁸ For more information about European EPC Competence Center (EECC) consult: <http://www.eecc.info/>.

²⁹ For more information about GS1 Germany consult: <http://www.gs1-germany.de/>.

³⁰ For more information about Deutsche Post World Net (DHL) consult: <http://www.dpwn.de/>.

³¹ For more information about Karstadt Warenhaus consult: <http://www.karstadt.de/>.

³² For more information about the METRO Group consult: <http://www.metrogroup.de/>.

³³ For more information about the International Standardization Organization (ISO) consult: <http://www.iso.org/>.

in publishing articles concerning the EPCglobal standards suite.

EPCglobal also works closely together with RFID Journal that as an independent media company was founded by its chief editor Mark Roberti in New York in March 2002 (RFID Journal, 2009b). RFID Journal devotes itself to covering news and updates regarding EPC and RFID business applications in a variety of industries and other developments related to RFID. RFID Journal also provides EPC RFID training courses for companies that want to incorporate RFID in their business processes. Furthermore, RFID Journal actively participates in organizing major EPC RFID industry events. For instance, RFID Journal together with EPCglobal organized the fifth annual EPC Connection Conference and Exhibition in Chicago from 14 until 16 October 2008.³⁵

4.2.3 Conclusion

This section showed that the regime insiders of the *incumbent traditional barcode regime (GSI-EAN/UPC)* set out to change the regime from within by setting up the *RFID technological niche (GSI-EPCglobal-EPC)*. The EPC network that consists of the Auto-ID labs, GS1global and its subsidiary EPCglobal, EECC and RFID Journal, carries the RFID technological niche. They together with their partners and members from industry and academia develop and promote the EPCglobal standards suite. The EPC network (EPC technology producers and users or EPC industry) propagates a constructive and positive business perspective in which EPC technologies have a huge potential to add value to businesses in a variety of industries. They perceive EPC technologies to benefit businesses and consumers, by providing better and or additional services and reducing prices for consumer products.

In retail, the current focus of the EPCglobal partners is to stimulate the adoption of the EPCglobal standards suite in the back-end Business-to-Business (B2B) supply chain domain (logistics) on pallets (pallet-level) and cases (case-level). The application of EPC on consumer products (item-level) in the front-end and in-store Business-to-Consumer (B2C) domain would be the next major step in the EPC evolution. Already, retailers together with their partners from industry have started RFID pilot projects in the *RFID technological niche* to explore the B2C application domain for EPC technologies. As we will see in the next sections, the EPC network met with fierce opposition from consumer privacy NGOs.

³⁴ For more information about RFID Journal consult: <http://www.rfidjournal.com/>.

³⁵ For more information about EPC Connection 2008 consult: <http://www.epcconnection.com/>.

4.3 EPC/RFID consumer privacy controversies in the EU and the US (Q2+Q4)

4.3.1 EPC/RFID consumer privacy controversies triggered by NGOs

Since the inception of EPCglobal in 2003, several retailers (technology users), together with RFID technology developers and system integrators (technology producers) have experimented with EPC on consumer products in RFID pilot projects. These field tests have received a lot of criticism and bad press (Thiesse, 2007). Consumer privacy and civil liberty NGOs revealed RFID misconduct by retailers and voiced their concerns for RFID and consumer privacy to the press. These publications resulted in consumer privacy controversies that rippled through the RFID industry, impeding upon the consumer acceptance and trust in RFID and EPC technologies. Table 7 below provides an overview of actions and reactions in consumer privacy controversies associated with the RFID pilot projects undertaken by Benetton³⁶ and Philips³⁷ in March 2003, Wal-Mart³⁸ and Gillette in July 2003, Tesco³⁹ and Gillette in July 2003.

Companies	Date	Events
Benetton/Philips	March 11, 2003	Action: Benetton announces that it plans to sew RFID into fabrics produced at Sisley. Two days later, in the internet, CASPIAN calls for a boycott of Benetton products
	April 9, 2003	Reaction: Benetton announces in a press release that it will not use RFID in textiles
Wal-Mart/Gillette	July 8, 2003	Action: CASPIAN publishes 68 “confidential” documents from the Auto-ID Center, which includes Wal-Mart and Gillette amongst its largest sponsors. On April 30, Wal-Mart had commenced an RFID pilot project for automated inventories in sales areas
	July 9, 2003	Reaction: Wal-Mart terminates the pilot project and announces that it will use RFID only in internal logistics
Tesco/Gillette	July 22, 2003	Action: the British retailing chain Tesco is accused of using RFID technology in order to capture data and photograph customers as they remove razor blades from a shelf
	Augustus 15, 2003	Reaction: Gillette denies all allegations, but Tesco admits to testing the “security-related advantages” of RFID technology. The pilot project is terminated at the end of July 2003

Table 7 - RFID consumer privacy controversies in retail (adapted: Thiesse, 2007: 221)

As table 7 shows, the consumer privacy and civil liberty NGOs play a key role in revealing consumer privacy issues with RFID in retail. The American grassroots consumer organization Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)⁴⁰, led by founder Katherine Albrecht, is the most fervent anti-RFID activist organization. Their mission is to inform the public about the severe dangers associated with the RFID technology.

³⁶ For more information about Benetton consult: <http://www.benetton.com/>.

³⁷ For more information about Philips consult: <http://www.philips.com/>.

³⁸ For more information about Wal-Mart consult: <http://walmartstores.com/>.

³⁹ For more information about Tesco consult: <http://www.tesco.com/>.

⁴⁰ For more information about Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) and its daughter Spychips consult: <http://www.nocards.org/> and <http://www.spychips.com/> respectively.

CASPIAN triggered these consumer privacy controversies by drawing attention of the press and by using the Internet as a key medium to voice their criticism to the public. For instance, CASPIAN launched boycott websites such as ‘www.boycotttestco.com’ and ‘www.boycottgillette.com’ to warn consumer about the dangers associated with the application of RFID in these field tests (see table 7 above). CASPIAN combines this with organizing onsite protests at retailers. CASPIAN equipped with these tools work together with for instance their German counterpart, the Association for the Promotion of Public Mobile and Immobile Data Traffic (FoeBuD).⁴¹ CASPIAN and FoeBuD triggered the consumer privacy controversy associated with the customer card in the METRO Group EXTRA Future Store in Rheinberg in 2004. The consumer privacy controversy at the Future Store will be extensively analyzed in section 4.4.

The next section will discuss the joint RFID Position Statement that CASPIAN and FoeBuD together with other major consumer privacy and civil liberty NGOs released in reaction to the field tests with RFID.

4.3.2 RFID Position Statement published by NGOs

On 20 November 2003, as a reaction to the RFID pilot projects and the consumer privacy controversies, almost fifty consumer privacy and civil liberties organizations (NGOs) led by CASPIAN and the Privacy Rights Clearhouse⁴² published a shared RFID Position Statement (CASPIAN, 2003). Among these NGOs were the prominent NGOs such as the Electronic Privacy Information Center (EPIC)⁴³, the Electronic Frontier Foundation (EFF)⁴⁴, the American Civil Liberties Union (ACLU)⁴⁵, and FoeBuD.

The RFID Position Statement specifically addresses the application of the Electronic Product Code (EPC) technology on consumer products in retail. Although EPC does not contain any personal data, the NGOs are concerned that the global uniquely identifiable EPC is coupled/linked with data retailers already aggregated such as data from customer loyalty cards, debit cards, or credit cards. In this way, the EPC has the potential to become personal data, i.e. a globally unique personal identifier for a customer. Furthermore, it is possible that RFID tags are read without consumer knowledge or consent. Not only by retailers or other private companies but also by the government and third parties that mean harm. Because of this ability of EPC on RFID tags to identify, track and trace consumers’ whereabouts, purchases, and possession, detailed consumer profiles can be aggregated without consumers’ being aware of it. Consequently, consumers become completely transparent, so-called ‘glass-consumers’. Even worse, consumers can be treated in accord with their aggregated consumer profiles, without even knowing their existence and how to correct them.

In order to mitigate consumer privacy and civil liberty risks, the NGOs in the RFID Position Statement call for several measures. They recommend RFID to be used only in the logistical B2B retail supply chain, because RFID is not exposed to consumers. Regarding the B2C domain, the consumer environment within the stores and beyond the point of sale they provide a list of RFID practices that should be prohibited. Furthermore, they call for a formal multi-disciplinary Technology Assessment (TA) by a neutral entity involving all stakeholders including consumers. Until the TA has been completed, the RFID Position Statement calls for a strong policy framework concerning RFID applications to protect the privacy and civil liberties of consumers. This policy framework needs to be based upon the Principles of Fair

⁴¹ For more information about the Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) consult: <http://www.foebud.org/>.

⁴² For more information about the Privacy Rights Clearhouse consult: <http://www.privacyrights.org/>.

⁴³ For more information about the Electronic Privacy Information Center (EPIC) consult: <http://epic.org/>.

⁴⁴ For more information about the Electronic Frontier Foundation (EFF) consult: <http://www.eff.org/>.

⁴⁵ For more information about the American Civil Liberties Union (ACLU) consult: <http://www.aclu.org/>.

Information Practice (PFIP) from the eight-part Privacy Guidelines stated in the ‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ adopted by the Organization for Economic Co-operation and Development (OECD)⁴⁶ on 23 September 1980 (OECD, 1980). According to the RFID Position Statement, the key principles that should be implemented for applications of EPC on consumer products are: openness or transparency, purpose specification, collection limitation, accountability and security safeguards.

4.3.3 Conclusion

This section showed that outside societal pressure groups (regime outsiders) offered critique on the RFID pilot projects conducted by EPC technology users and producers (regime insiders) within the *RFID technological niche (GSI-EPCglobal-EPC)*. By using the press, the consumer privacy and civil liberty NGOs pointed out the consumer privacy issues with the EPC technology. They worry about privacy loss for consumers in EPC/RFID enabled applications on consumer products in the retail sector. According to the NGOs, RFID in this application domain entails an unprecedented threat to consumer privacy and their civil liberties. Retailers, governments or other parties have the ability of ubiquitous surveillance of customers’ movements and purchases and hence the ability to establish elaborate consumer profiles. Therefore, the NGOs call for forbidding certain use, an official Technology Assessment (TA) to identify the risks, and sound regulations to mitigate the potential negative consequences of RFID for consumer privacy and their civil liberties.

⁴⁶ For more information about the Organization for Economic Co-operation and Development (OECD) consult: <http://www.oecd.org/>.

4.4 The METRO Group Future Store Initiative phase one (METRO 1) (Q1-Q4)

4.4.1 The establishment of the METRO Group Future Store Initiative⁴⁷

The METRO Group⁴⁸ is Germany's largest and the world's third largest retailer. Together with about sixty partner companies, they started their innovation journey of RFID by founding the METRO Group Future Store Initiative (MGFSI) in July 2002. The MGFSI is an initiative for establishing a real-life RFID driven joint Research & Development (R&D) platform. The mission of the MGFSI is to define the standards of the future of retailing using innovative technologies. Figure 17 below depicts the major partner companies of the MGFSI as of June 2004. The METRO Group had the unquestionable leadership role in the network of partner companies in the MGFSI. The collaboration practices of the METRO Group and its partner companies led up to the realization of the EXTRA Future Store in Rheinberg only seven months after its foundation.

Figure 1: Major Partners in the METRO Group Future Store Initiative ³	
FSI Partners	
Technology <ul style="list-style-type: none"> • Intel (www.intel.com) • IBM (www.ibm.de) • AlgoTec (www.algotec.de) • Bizerba (www.bizerba.de) • Checkpoint (www.checkpointeurope.com) • Cisco (www.cisco.de) • Feig (www.feig.de) • Fujitsu Siemens (www.fujitsu-siemens.de) • Hewlett Packard (www.hewlettpackard.de) • Intermec (www.intermec.de) • Liebherr (www.liebherr.de) • Mettler Toledo (www.mt.com) • MultiQ (www.multiq.com) • NCR (www.ncr.com) • Philips (www.philips.com) • Sonopress (www.sonopress.de) • Symbol (www.symbol.com) • Wincor Nixdorf (www.wincor-nixdorf.com) 	Services <ul style="list-style-type: none"> • Alpha (www.alpha-erding.de) • Avery Dennison (www.averydennison.com) • BCG (www.bcg.com) • CHEP (www.chep.com) • Cittadino (www.cittadino.de) • DHL (www.dhl.de) • Eyckeler & Malt (www.eyckeler.com) • Hintzpeter & Partner (www.hintzpeter.de) • Kurt Salmon Associates (www.kurtsalmon.com) • Loyalty Partner (www.loyaltypartner.com) • VISA (www.visa.de) • Wanzl (www.wanzl.de) • WMS (www.wms.net)
Software <ul style="list-style-type: none"> • SAP (www.sap.com) • Microsoft (www.microsoft.com) • OAT System (www.oatsystems.com) • Online Software (www.online-gmbh.de) • Oracle (www.oracle.de) • Pironet NDH (www.pironet-ndh.com) 	Brands <ul style="list-style-type: none"> • Coca-Cola (www.coca-cola-gmbh.de) • Gillette (www.gillette.de) • Henkel (www.henkel.de) • Johnson & Johnson (www.jnjgermany.de) • Kraft Foods (www.kraftfoods.de) • Nestlé (www.nestle.de) • Procter & Gamble (www.procterundgamble.de)

Figure 17 - Major partner companies of the MGFSI as of June 2004 (Loebbecke, 2004: 178)

⁴⁷ This section is a synthesis based upon: Loebbecke, 2004; Loebbecke, 2005; Graczewski and Man, 2006.

⁴⁸ For more information about the METRO Group consult: <http://www.metrogroup.de/>.

4.4.2 The EXTRA Future Store and its RFID applications⁴⁹

On 28 April 2003, the MGFSI opened the Extra Future Store, a bricks-and-mortar supermarket in Rheinberg near Düsseldorf, the capital of the Germany's federal state Nordrhein-Westfalen (NRW). 'EXTRA' belonged to the METRO Groups EXTRA supermarket chains. In the Future Store the METRO Group experiments in a real-life setting with state-of-the-art ambient technologies that aim at enriching the shopping experience of their customers. In the Future Store the METRO Group and its partners want to investigate how consumers and employees respond and preferably accept new innovative technologies in retail. To enable a full self-service shopping trip, the MGFSI pioneered, supported by a Wireless Local Area Network (WLAN) and the back-end IT infrastructure, the following ambient technologies in the Future Store. For faster and more convenient shopping the personal shopping assistance, self-checkouts, and intelligent weighing scales (smart scales) were pioneered. For enhanced communication with the customer, personalized digital advertising displays, interactive kiosks (web based information terminals), and electronic price tags were pioneered.

Another key innovative ambient technology that was pioneered in the Future Store was the application of the RFID technology on groceries and was the first and largest rollout of the EPC technology in Europe. The purpose of experimenting with RFID was developing new standards and processes in managing consumer products in the retail value chain, stretching from production, distribution, sales, and beyond. Beyond refers to the potential future use of RFID tagged consumer products in household applications such as intelligent refrigerators, intelligent washing machines, and intelligent wine cabinets. In short, the purpose of the MGFSI was to learn how to use and produce the RFID technology in the retail supply chain. Consequently, a big part of Future Store was devoted to the RFID pilot project in which four consumer products were individually tagged with RFID. These products were 'Philadelphia cream cheese' by Kraft Food, 'Pantene Pro V Shampoo' by Proctor & Gamble, 'Mach 3 Turbo razorblades' by Gillette, and CDs, DVDs, and videos. Additional to these in-store applications, the supply chain management was included as well. In the back-end of the Future Store, RFID tags were attached to pallets, crates, and boxes. RFID readers were mounted on dock doors and other transshipment points in the Future Store.

Improving the inventory management system was the main goal. To illustrate, Kraft Food wanted to gain experience with the management of expiration dates and out of stocks. Proctor & Gamble wanted to experiment with innovative marketing concepts using advertising displays for their Pantene Shampoo. Gillette wanted to experiment with anti-theft protection for their razor blades. All these three RFID tagged consumer products were stored on smart shelves that were equipped with bottom-integrated RFID readers. These shelves were able to read their contents by reading the RFID tags of the consumer products that they stored. The shelves were able to synchronize this information with inventory management system of the Future Store. Consequently, aiming at reducing out of stocks, store employees could be notified when the shelves needed to be replenished. Additional functionalities of the smart shelves were the prevention of misplaced consumer products and quality control by making sure that they only contained consumer products before their expiration date.

In the media terminal in the media department of the Future Store, before a customer was able to watch a movie trailer or listen to a music sample, his/her age needed to be checked. German law prescribes this procedure, as some movies are only eligible to be watched by persons older than sixteen. The media terminal checked the person's age by comparing the information stored on the RFID tagged CDs, DVDs, or videos, with the

⁴⁹ This section is a synthesis based upon: Kalyanam et al., 2006; Loebbecke, 2004; Loebbecke 2005; Hof and Cornelissen, 2006; Hof, 2007; RFID Journal, 2003; METRO Group, 2003.

PAYBACK number stored on what later appeared to be the controversial RFID enabled EXTRA Future Card. The EXTRA Future Card was the customer loyalty card of the Future Store that is part of the PAYBACK customer loyalty card program in Germany.⁵⁰ Since PAYBACK cards are only issued to persons of 16 years and older, checking the person's age was an easy procedure.

The kind of RFID tags that were used in the Future Store were passive read-only RFID tags. These were operating on High Frequency (HF) 13.56 MHz and had a read range of about 1.5 meters. These tags were equipped with I-Code microchips manufactured by Philips. These tags had incorporated theft protection to prevent shoplifting, comparable with the 'Electronic Article Surveillance' (EAS) devices used in retail today. This implied that the exit ports of the Future Store were able to detect whether RFID tagged consumer products were paid for when leaving the store. These HF RFID tags have a coiled antenna and work with 'magnetic induction' to communicate with the readers. To uniquely identify consumer products, the RFID tags stored the Global Trade Identification Number (GTIN) and a serial number, the predecessor of the EPC issued by EPCglobal. Before being embedded in the EPC infrastructure, the RFID tags were attached to the consumer products at the backroom of the Future Store or at the Distribution Center (DC) that supplied the Future Store.

4.4.3 The consumer privacy controversy at the EXTRA Future Store⁵¹

On 24 October 2003, FoeBuD awarded the METRO Group the 'Big Brother Award' in the category consumer protection (FoeBuD, 2003). This award is a so-called 'negative prize', as FoeBuD perceived the practices of the METRO Group's RFID pilot project in the Future Store and their aspirations concerning the rollout of RFID to impede upon consumer privacy. In addition, the METRO Group did not comply with the demands as crystallized in the joint RFID Position Statement that was published by major consumer privacy and civil liberty NGOs, as discussed in section 4.3.2.

On 31 January 2004, Rena Tangens and padeluun from FoeBuD together with Katherine Albrecht from CASPIAN and representatives from the press, took an official guided tour in the Future Store in Rheinberg. Besides offering the Big Brother Award to the METRO Group, FoeBuD wanted to show CASPIAN the RFID pioneering activities. Consequently, the MGFSI received the most critical visitors in their Future Store ever since. The guided tour went smoothly except for the fact that the deactivator beyond the point of sale at the exit of the store did not function as it was supposed to. The deactivator was meant for customers to deactivate RFID tags on the tagged consumer products in the Future Store. However, the deactivator only overwrote the EPC number on the RFID tags with zeros and left the globally hardcoded unique manufacturer serial number of the RFID tag intact. Consequently, the RFID tag was still active and could function as a unique identifier by being linked to a person and hence become personal data. At the end of the guided tour, FoeBuD offered the Big Brother Award, but the METRO Group representatives refused to accept it.

The next day on 1 February 2004, during the presentation of Katherine Albrecht from CASPIAN on RFID, members of FoeBuD accidentally discovered that the EXTRA Future Card contained an RFID chip that stored the PAYBACK customer number. This revelation allowed for the speculation that the METRO Group and other retailers that were also using the PAYBACK card to spy on their customers. The crux was that the customer card could function as a personal identifiable object, readable by RFID readers in the Future Store and elsewhere without customers consent. As a result, the PAYBACK customer card could be used for building consumer profiles, by tracking customers' movements and scanning their

⁵⁰ More information about the PAYBACK customer loyalty card program consult: <http://www.payback.de/>.

⁵¹ This section is a synthesis based upon: Hof and Cornelissen, 2006; Hof, 2007; Holland-Letz, 2006; FoeBuD, 2003; FoeBuD, 2004; CASPIAN, 2004, and the interview with Rena Tangens (FoeBuD) on 21 July 2008.

purchases. Even worse, malicious third parties outside the Future Store also had the opportunity to read the tags and scan the whereabouts and purchases of customers. Above all, the main frustration of FoeBuD and CASPIAN was that the METRO Group did not properly inform their customers about the RFID tag in PAYBACK customer card. There were many opportunities for doing this, for instance during guided tours, the RFID information brochure of the Future Store, and the application form of the PAYBACK customer card. Hence, FoeBuD and CASPIAN sought press attention and notified the METRO Group about the privacy intrusion of the RFID tagged PAYBACK customer card upon their customers.

Later that month on 27 February 2004, the METRO Group announced in email correspondence with FoeBuD and CASPIAN that they would replace the 10.000 circulating RFID tagged EXTRA Future cards with conventional bar-coded ones. The METRO Group decided to do this because of the bad press and consumer pressure on the use of RFID in the Future Store and in particular concerning the PAYBACK customer cards. It took the METRO Group about one month to replace the 10.000 PAYBACK customer cards. The cost for the METRO Group was estimated between 5.000 and 10.000 euro, considerably less than when this case would have been taken to court. Furthermore, the DVDs, CDs and videos media terminal for which the RFID tagged payback cards were used was replaced with a barcode reader. On the bar-coded EXTRA Future card, the PAYBACK card number is stored on the magnetic strip, contained in the barcode, and in human readable code at the back of the card. The media terminal therefore kept the same functionality of checking the age of the customer who wanted to see a movie trailer or listen to a music sample. Interestingly, both FoeBuD and CASPIAN reported that the METRO Group tried to cover up their negligence of informing the customers that RFID was employed in the PAYBACK customer card. The METRO Group denied all allegations by stating that customers were informed orally about their RFID use in the PAYBACK customer and about the other RFID applications elsewhere in the Future Store. This final dispute ended in a stalemate, however stimulating FoeBuD and CASPIAN to continue with their anti-RFID campaign entitled: 'Stop RFID'.

On 28 February 2004, FoeBuD demonstrated in front of the Extra Future Store in Rheinberg against the use of RFID by the METRO Group. During the demonstration, FoeBuD and their supporters warned customers of the Future Store about the dangers associated with RFID. Furthermore, the protest was meant to let the METRO Group know that they should abandon their RFID practices on individual consumer products. FoeBuD with their recently launched anti-RFID campaign was not satisfied by the METRO Group's withdrawal of the EXTRA customer cards. The METRO Group continued their RFID pilot project and thereby did not pay attention to the NGOs shared RFID Position Statement. Hence, to enforce their intentions and to show that they were serious, FoeBuD decided to proceed with the protest in the context of their anti-RFID campaign.

4.4.4 Call for RFID-specific regulation to accommodate consumer privacy concerns⁵²

According to Daniel Kitscha of Communication and Public Affairs of the METRO Group, 'All RFID deployments have been in full compliance with applicable legal provisions. Prevailing German and European privacy legislation covers all former and existing RFID applications at METRO Group.' The referred to RFID applications include the RFID pilot project activities of the METRO Group in the Future Store in Rheinberg in January 2004. Note that this is at the time of the consumer privacy controversy of the RFID tagged PAYBACK customer card and the malfunctioning deactivator. In 2004, only technology-neutral consumer privacy regulations were developed in Germany and in the European Union

⁵² This section is based upon email correspondence with Friedrich Thiesse (Auto-ID Labs University of St. Gallen) and Daniel Kitscha (METRO Group Information Technology (MGI)).

(EU) (see next chapter for more details). Following the statement of Kitscha, most likely the METRO Group did implement those in the Future Store in 2004. Nevertheless, according to Friederic Thiesse, associate director of the Auto-ID lab of the University of St. Gallen, 'privacy was not perceived as a relevant issue at the time when the first Future Store trial was started.' Thiesse could even recall a statement from a METRO Group executive in 2002/2003 who stated something like 'privacy is an American issue, not relevant to Europe.' This points out that the consumer privacy in relation to RFID was not on the agenda of the METRO Group and the EPC industry in Europe initially. Not surprisingly therefore that the consumer privacy controversy arose. By no means, RFID-specific consumer privacy regulation could have been implemented at the METRO Group Future Store in 2004.

Only after the bad press concerning the RFID activities and consumer privacy at the Future Store, consumer privacy was put on the agenda of the METRO Group and the EPC industry. The METRO Group learned the hard way, as it had to replace the PAYBACK customer cards with traditional bar-coded ones. In addition, the METRO Group installed and later improved the RFID tag deactivator beyond the point of sale at the exit of the Future Store. According to Thiesse, the first RFID transponders/tags that were used at the Future Store could not be deactivated permanently. The kill commando was not part of the EPC protocol specification in 2004 and hence not implemented in the RFID tags. The kill commando for the permanent deactivation of RFID tags became available in the EPC Generation 2 protocol specification at the end of 2005 and in the actual RFID tags/transponders available on the market in 2006. This leads to the conclusion that the deactivator in the Future Store at the time of the guided tour by FoeBuD and CASPIAN in January 2004, was indeed malfunctioning and misleading as described above. According to Thiesse, these initial issues with consumer privacy at the Future Store was a sign for the EPC industry, including the METRO Group, to 'cooperate with policy makers on the national and the EU level.' Thus, the METRO Group and the EPC industry learned the hard way and adjusted their course accordingly. The EPC industry realized that to accommodate consumer privacy concerns associated with RFID in this new application domain of consumer products, RFID-specific regulations needed to be developed together with policy makers on the national and European level.

Despite the negative publicity triggered and uttered by NGOs and the press concerning the RFID activities undertaken by the METRO Group, they did not abort it. According to Thiesse there are two main reasons. The first reason was that the criticism on RFID voiced by the NGOs and magnified by the press beyond proportions did not catch on to the larger public (see also Thiesse, 2007). Secondly, the benefits that were expected from RFID were estimated too high as well. Consequently, the METRO Group focused more on the application and gains of RFID in the retail supply chain, instead of the consumer application domain. In November 2004, the METRO Group separated their RFID activities in the B2B supply chain and their RFID activities on consumer products in the Future Store. From then on, together with its suppliers the METRO Group focused on the gradual rollout of RFID in the B2B supply chain on pallets, boxes, crates, and cases.

In retrospect, although pivotal, the consumer privacy controversy in the early days of the Future Store in Rheinberg should be placed into perspective. According to Kalyanam et al. (2006), the technological innovation pioneering activities in the Future Store led to an increase in customer satisfaction. Consequently, the increased customer satisfaction was translated into more loyal customers that wanted to shop frequently at the Future Store. Furthermore, in a period of four years, the Future Store in Rheinberg drew 31.000 visitors from 93 nations for guided tours (MGFSI, 2009). Thus, the MGFSI with their Future Store in Rheinberg showed the world innovative technologies in retail and no doubt drew considerable

attention in doing so. Above all, the MGFSI learned from their early mistakes in the Future Store and adjusted their course accordingly.

4.4.5 The METRO Group RFID Innovation Center and its RFID applications⁵³

On 7 July 2004, in addition to the Future Store in Rheinberg, the MGFSI established the RFID Innovation Center located in Neuss near Düsseldorf in Germany. The RFID Innovation Center is a real-life RFID exhibition lab in which contemporary and near future RFID related technologies are exhibited to the public. Furthermore, it functions as a research lab for partner companies of the MGFSI as they are able to test and exchange experiences with innovative RFID related technologies. Covering about 2000 square meters, the RFID Innovation Center presents innovations in as well the B2B back-end supply chain, the B2C front-end CPILT application domain, their integration, and beyond the point of sale. In the RFID Innovation Center the following five application domains of RFID are exhibited: order picking, warehouse management, department stores, store of the future, and at home.

The last category 'RFID at home' is interesting as it is the most far out category. In the RFID Innovation Center, partly functioning prototypes of RFID enabled future household appliances are exhibited. One of such an appliance is the intelligent washing machine that washes clothes according to the information on the RFID tag that is sewed in the garments. Another application is the intelligent refrigerator that is able to scan the RFID tagged consumer products. As a result, the smart fridge can indicate on the attached flat screen its content and when products have expired and need to be reordered at the retailer for replenishment. The exhibition also includes the intelligent wine cabinet that on a flat screen is able to indicate its contents. These household applications could stimulate the demand for RFID tagged consumer products, i.e. creating the pull-effect for CPILT.

At the end of 2005, the European EPC Competence Center (EECC), although an independent RFID testing facility for EPCglobal, was co-housed in the same building as the METRO Group RFID Innovation Center. Both are located in Neuss, in a Distribution Center (DC) for the Galeria Kaufhof⁵⁴ department store division of the METRO Group. This indicates once again the close link between the METRO Group, EECC, and EPCglobal on the local level in Nordrhein-Westfalen (NRW) in Germany.

⁵³ This section is a synthesis based upon: Collins, 2004; METRO Group, 2004; MGFSI; 2009, and the guided tour I took at the METRO Group RFID Innovation Center on 04 July 2008.

⁵⁴ For more information about Galeria Kaufhof consult: <http://www.galeria-kaufhof.de>.

4.4.6 Conclusion

This section described the socio-technical configuration of the RFID pilot projects of the METRO Group Future Store Initiative (MGFSI) phase one, ‘METRO 1’, in the *RFID technological niche (GSI-EPCglobal-EPC)*. The R&D network of companies that participate in the MGFSI set out to learn how to *use* and *produce* the RFID technology on individual consumer products (regime insiders). Furthermore, this section showed the consumer privacy controversy associated with the PAYBACK customer card and the malfunctioning deactivator in the first RFID pilot project of the MGFSI, i.e. the Future Store in Rheinberg (METRO 1). The consumer privacy controversy was triggered by societal pressure groups in the embodiment of consumer privacy NGOs FoeBuD and CASPIAN (regime outsiders). After the consumer privacy controversy of ‘METRO 1’, the METRO Group and the EPC industry took consumer privacy in relation to RFID seriously and it was to occupy a prominent place on the RFID agenda from then onwards. In other words, the METRO 1 consumer privacy controversy marks the first steps in the learning process of how to *regulate* RFID for tagging individual consumer products (CPILT) in the retail sector.

The MGFSI on a local level is the *locus* for which and in which the first RFID-specific regulations will be developed, imposed upon, implemented, and consequently manifest themselves to the public. Hence, in this study the MGFSI with its Future Store and RFID Innovation Center is considered the local level of the emerging governance regime for consumer privacy protection of RFID in retail. This governance regime for consumer privacy protection will yield RFID-specific regulation to accommodate the emerging RFID application on consumer products. Consequently, these are imposed upon RFID enabled applications such as the RFID pilot projects of the MGFSI. Figure 18 below depicts this local level arena of the emerging governance regime for consumer privacy protection. The MGI is the METRO Group Information Technology department that is the national and international IT service provider for all companies of the METRO Group.⁵⁵ Consequently, the MGI facilitates and is responsible for running the MGFSI.

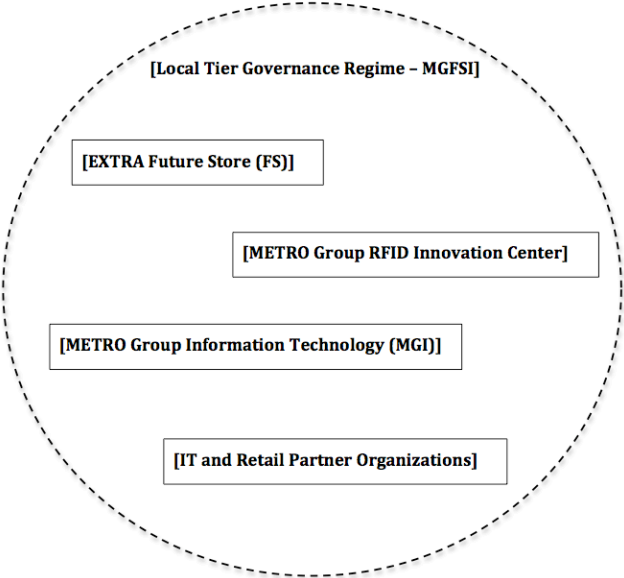


Figure 18 - Local tier arena of the emerging governance regime for consumer privacy protection

⁵⁵ More information about the METRO Group Information Technology (MGI) consult: <http://www.mgi.de/>.

4.5 The voluntary EPC industry self-regulation initiative⁵⁶ (Q2+Q4)

4.5.1 The EPCglobal Guidelines on EPC for Consumer Products

Following the consumer privacy controversies and the shared RFID Position Statement of the civil liberties and consumer privacy NGOs, EPCglobal started to address consumer privacy issues associated with the EPC technology. EPCglobal published the ‘EPCglobal Guidelines on EPC for Consumer Products’ on 1 January 2005 (EPCglobal, 2005).

The EPCglobal Guidelines prescribe the following five principles to the EPC member organizations that employ the EPC technology in applications for consumer products. Firstly, consumers should be given clear notice when EPC is used on consumer products. Secondly, consumers should be informed about the choices they have regarding the use and removal of EPC after purchase. Thirdly, consumers should be educated about EPC and its applications. Finally, companies that employ EPC should protect and maintain data generated by EPC conform the applicable legislations.

With the EPCglobal Guidelines, EPCglobal aims at a responsible use of the EPC technology by all the companies that comply with the EPCglobal standards suite. Members of EPCglobal must subscribe to these Guidelines by implementing them in their RFID enabled applications when consumers are exposed to EPC, e.g. in RFID pilot projects operated by the MGFSI. Furthermore, EPCglobal is responsible for seeing to it that companies that employ EPC technology abide the EPCglobal Guidelines. EPCglobal is also responsible for reviewing and updating the EPCglobal Guidelines as the EPC technology develops and matures.

4.5.2 Background of the EPCglobal Guidelines

The EPCglobal Guidelines have their roots at the MIT Auto-ID Center discussed in section 4.2.1. The leadership of the Auto-ID Center instituted an independent International Public Policy Advisory Council (PPAC) to assist them in policy issues, of which consumer privacy was the most important one. The PPAC consisted of privacy experts from Europe, Japan, Australia, and US. The members of the PPAC had close ties with governments, academic experts, and NGOs. Several of them even served in senior governmental positions, or had positions of authority in academic and professional organizations that dealt with privacy issues. The Auto-ID Center’s leadership together with the PPAC decided that it would be appropriate to draw up Guidelines for the EPC technology users on how to implement the EPC technology in a responsible way. Although EPC is a neutral technology, the Guidelines were envisioned to rule out any societal unacceptable use of the EPC technology and hence stimulate its adoption for its benefits to be reaped.

The Auto-ID Center instituted a drafting committee that had the task of putting together the envisioned Guidelines. The discussions and drafting process of the Guidelines by the drafting committee and the PPAC were not public. They believed that private discussions would stimulate open discussions and the exchange of viewpoints concerning consumer privacy and RFID. As the focus on consumer privacy was clear from the beginning, the drafting committee turned to the well-established and endorsed privacy principles in the OECD Privacy Guidelines (OECD, 1980) for policy guidance. The OECD Privacy Guidelines reflect consensus (balanced interest) concerning privacy amongst governments, industry, and civil society of the OECD member countries. Subsequently, there were multiple cycles of discussions and drafts amongst the drafting committee, the Auto-ID Center’s board and its member organizations. The member organizations of the Auto-ID Center were asked to discuss the draft internally and with their own stakeholders, including responsible legal and

⁵⁶ This section is a synthesis based upon: EPCglobal, 2009c, and email correspondence with Elizabeth Board (EPCglobal).

privacy officials. Simultaneously, the PPAC analyzed the proposed draft in the light of past practices and literature on the introduction of new technologies. The members of the PPAC also consulted with their local privacy authorities, governments, public interest groups, and academic experts. Consequently, the members of the PPAC came together a couple of times to discuss their findings concerning the proposed draft. Then the PPAC communicated their detailed findings in a recommendation to the drafting committee. The drafting committee did not fully appreciate the recommendation provided by the PPAC, as it did not fully represent the interest of the Auto-ID Center. This is explained by the fact that the PPAC was an independent advisory group that provided an independent perspective on the proposed Guidelines. After several discussions with the Auto-ID Center's board, the Guidelines were adopted and passed on to EPCglobal once it was established in 2003.

4.5.3 Maintenance of the EPCglobal Guidelines

Early 2004, EPCglobal instituted a multi-industry and global Public Policy Steering Committee (PPSC) with representatives from industry and trade organizations (EPCglobal, 2009c). Among its members are: Gillette, Procter & Gamble, Nestle⁵⁷, Unilever⁵⁸, Johnson & Johnson (J&J)⁵⁹, METRO Group, Ahold⁶⁰, Carrefour⁶¹, Tesco, DHL, Philips, Association for Automatic Identification and Mobility (AIM)⁶², European Retail Round Table (ERRT)⁶³ and GS1global. The purpose of the PPSC is to engage in open dialog with key stakeholders in the public and private sector to address public policy issues such as consumer privacy in relation to EPC.

The PPSC is responsible for the maintenance of the 'EPCglobal Guidelines on EPC for Consumer Products' published on 1 January 2005 (EPCglobal, 2005). The PPSC instituted a subcommittee to regularly review and address issues related to the EPCglobal Guidelines. Examples of new developments are the Privacy Impacts Assessments (PIA), new types of EPC applications, and changes in technological developments. The subcommittee reports to the PPSC that in turn is responsible for maintaining and providing additional guidance to keep the public policy process for EPC abreast. The PPSC in turn reports to EPC Board of Governance (EPCglobal, 2009a).

Since their publication in 2005, besides *internally* in EPCglobal and among its partner organizations the EPCglobal Guidelines have been discussed *externally* in forums organized by the US Federal Trade Commission (FTC), the US Department of Commerce, the European Commission, and consumer groups. However, the EPCglobal Guidelines underwent minor changes that primarily had editorial or clarification purposes.

To support the EPCglobal Guidelines the PPSC collaborated with the National Consumer League (NCL) to set up a website "www.DiscoverRFID.org" to educate consumers about the benefits of RFID (not only EPC). The PPSC also developed a 'Retailer Tool Kit' to assist retailers in informing their employees and customers about the EPC/RFID technology.

⁵⁷ For more information about Nestle consult: <http://www.nestle.com/>.

⁵⁸ For more information about Unilever consult: <http://www.unilever.com/>.

⁵⁹ For more information about Johnson & Johnson (J&J) consult: <http://www.jnj.com/>.

⁶⁰ For more information about Ahold consult: <http://www.ahold.com/>.

⁶¹ For more information about Carrefour consult: <http://www.carrefour.com/>.

⁶² For more information about Association for Automatic Identification and Mobility (AIM) consult: <http://www.aimglobal.org/>.

⁶³ For more information about the European Retail Round Table (ERRT) consult: <http://www.errt.org/>.

4.5.4 Conclusion

This section showed that the EPC technology producers and users (regime insiders) in the *RFID technological niche (GSI-EPCglobal-EPC)* devised the EPCglobal Guidelines as the voluntary (private) industry self-regulation initiative or code of conduct for the EPC industry (EPC technology users and producers). This after the consumer privacy issues with the EPC technology in the RFID pilot projects that were revealed by the societal pressure groups (regime outsiders).

The EPCglobal Guidelines harmonize with existing technology-neutral national and international consumer privacy legislations, regulations, and guidelines. The main reason for this is that the EPCglobal Guidelines are based upon the widely endorsed OECD Privacy Guidelines (OECD, 1980). Secondly, the EPCglobal Guidelines have been extensively discussed *internally* in EPCglobal (former Auto-ID Center) and among their partner organizations, and *externally* in open forums organized by governmental organizations and privacy organizations. The EPC Guidelines therefore mark the kickoff of the RFID-specific regulation for the application of RFID on consumer products in the retail sector.

With the Guidelines, EPCglobal pursued to provide an answer to the growing societal consumer privacy concerns of RFID applied on consumer products. They seem aware of the fact that the success of EPC depends on consumers' trust and acceptance of the EPC technology. The EPCglobal Guidelines can be considered far reaching measures to warrant consumer privacy in EPC enabled applications. Nevertheless, the Guidelines have proven not to be the answer to the societal privacy concerns concerning RFID. As what will become clear in the next chapter, the EPCglobal Guidelines form the basis for additional RFID-specific regulations to warrant consumer privacy and stimulate consumers' trust and acceptance of the EPC technology.

4.6 Conclusion

After the consumer privacy controversy of the METRO Group's first RFID pilot project in Rheinberg Germany in 2004 (METRO 1), a lot has changed in the RFID landscape. From an industry perspective, EPCglobal with its partners intensified their initiatives concerning the technological *standardization* of how to *use* and *produce* their global and multi-industry EPC standards suite in the *RFID technological niche (GS1-EPCglobal-EPC)*. From a policy perspective, a lot has taken place regarding the development of consumer privacy regulation for RFID. We already saw that the METRO Group's and the other consumer privacy controversies in retail triggered voluntary industry self-regulation in the embodiment of the 'EPCglobal Guidelines for EPC on Consumer Products'. Table 8 below depicts a comprehensive overview of the most important outcomes, processes, and involved institutions that led up to the EPCglobal Guidelines.

The next chapter of the RFID governance case study will show that METRO 1 kicked off a further policy debate about RFID and consumer privacy in Germany, Europe, and beyond. In recent years, there have emerged continuous policy processes yielding policy outcomes for the regulatory framework for consumer privacy protection of RFID. In other words, *learning* took place of how to *regulate* the application of RFID on consumer products in the retail sector. These policy outcomes are the result of heterogeneous (industrial, societal, science, politico-administrative) stakeholders, each having different perspectives, interacting with each other in connected multi-tier (local, regional, national, transnational and international) policy arenas.

Year	Outcomes	Processes	Institutions/Organizations	Interpretation
1999	- Auto-ID Center	- Founding of the Auto-ID Center	- MIT, UCC, Proctor & Gamble, Gillette, and partners from industry	- Academic spin-off, working with industry on R&D of RFID, marks the birth of RFID for retail
2002	- RFID Journal - MGFSI	- Founding of RFID Journal - Founding of the METRO Group Future Store Initiative (MGFSI)	- RFID Journal - METRO Group, IT and Retail partners (~60 in total)	- Global RFID industry Journal that promotes the EPC - First RFID-driven R&D platform in the retail sector in Germany
2003	- Auto-ID labs - EPCglobal - Consumer privacy controversies in EU and US - MGFSI opens Future Store in Rheinberg (METRO 1) - Publication of RFID Position Statement by NGOs	- Transition completed from Auto-ID Center to a global Auto-ID labs network to conduct R&D towards RFID - Foundation of EPCglobal as a global and multi-industry commercial organization managing the EPC standards suite - NGOs reveal consumer privacy issues with RFID applied on consumer products (CPILT) at major retailers - The opening of the Future Store (METRO 1), a RFID pilot project for learning how to use and produce EPC/RFID on CPILT under real-life conditions (5 consumer products are tagged) - NGOs in US/EU publish a shared position statement on RFID	- Auto-ID labs network - Auto-ID labs, UCC, EAN International and major partners from industry (incl. METRO Group) - Benetton/Philips, Walmart/Gillette, and Tesco/Gillette - METRO Group, IT and Retail partner organizations (MGFSI) - CASPIAN, Privacy Rights Clearhouse, EPIC, EFF, ACLU FoeBuD and more	- Academia/Industry R&D to RFID goes global - The EPC standards suite as an RFID standard is promoted as the successor of the EAN/UPC barcode standard in retail to be managed by EPCglobal - RFID applied on consumer products (CPILT) is problematic for consumer privacy - METRO 1 is the first field test with RFID/EPC on consumer products (CPILT) in Germany - Transatlantic NGOs join forces as they perceive RFID/EPC on CPILT to be harmful for consumer privacy
2004	- METRO 1 consumer privacy controversy	- NGOs FoeBuD and CASPIAN discover that the customer card contains an RFID tag, causing bad press and a demonstration in front of the Future Store (METRO 1). The METRO Group resigns and replaces 10.000 customer cards with conventional	- METRO Group, IT and Retail partner organizations (MGFSI), FoeBuD, CASPIAN and the press.	- Birth of the consumer resistance towards the application of RFID/EPC on consumer products in retail. This marks the birth of the

	<ul style="list-style-type: none"> - EPCglobal institutes a Public Policy Steering Committee (PPSC) - MGFSI opens METRO Group RFID Innovation Center 	<p>bar-coded ones. Deactivator at exit of the Future Store is malfunctioning.</p> <ul style="list-style-type: none"> - EPCglobal institutes a global multi-industry Public Policy Steering Committee (PPSC) to address public policy issues of EPC/RFID. - The founding of a real-life exhibition lab with current and potential near future application domains of RFID in retail (B2B and B2C) 	<ul style="list-style-type: none"> - PPSC of EPCglobal, partners from industry (incl. METRO Group) - METRO Group and IT and Retail partners (MGFSI) 	<p>policy process for RFID-specific regulation on the National and EU level (how to regulate RFID on CPILT)</p> <ul style="list-style-type: none"> - The EPC industry takes public policy issues concerning EPC seriously (especially consumer privacy) - METRO Group and its partners in the MGFSI expand the RFID driven R&D platform in retail.
2005	<ul style="list-style-type: none"> - GS1global - First RFID-specific regulation: The EPCglobal publishes 'EPCglobal Guidelines on EPC for Consumer Products' - EECC 	<ul style="list-style-type: none"> - Founding of GS1global and EPCglobal becomes its subsidiary - EPCglobal publishes industry-self regulation to address consumer privacy issues for the application of EPC on consumer products (CPILT) - Founding of the European EPC Competence Center (EECC), co-housed with the METRO Group RFID Innovation Center 	<ul style="list-style-type: none"> - GS1global, UCC and EAN International - EPCglobal and partner organizations in the EPC network - GS1-Germany (representative EPCglobal), DHL, METRO Group, Karstadt 	<ul style="list-style-type: none"> - Global barcode (EAN/UPC) and EPC standard managed by one organization - EPC industry takes consumer privacy seriously and takes matters in their own hands. It marks the first RFID-specific regulation (industry self-regulation) - EPCglobal is well-established in the German retail industry

Table 8 - Overview outcomes, processes, and involved institutions in the development of RFID-specific consumer privacy regulation between 1999 and 2005

5. RFID governance case study part two – The emerging RFID-specific regulatory capability for consumer privacy protection in retail

5.1 Introduction

This chapter covers the second part of the RFID governance case study of the European Union (EU), and answers the conceptual-laden research questions Q1-Q4. Again, the analysis is centered on the METRO Group Future Store Initiative (MGFSI). As showed in part one of the RFID governance case study, the MGFSI has been conducting RFID pilot projects on Consumer Product Item-level Tagging (CPILT) in the front-end and in-store Business-to-Consumer (B2C) application domain in the retail sector since 2003. Following the ‘METRO 1’ consumer privacy controversy of January 2004, this chapter will analyze the regulatory capability for consumer privacy protection of RFID in retail that emerged between 2005 and 2008. The regulatory capability is the emerging governance regime that consists of multi-actor (industrial, societal, science, politico-administrative) and multi-tier (local, regional, national, transnational, international) regulatory processes yielding RFID-specific consumer privacy regulations. These RFID-specific regulations are developed against the backdrop of the established technology-neutral consumer privacy legislations and regulations. Subsequently, the RFID-specific consumer privacy regulations are imposed upon ‘METRO 2’, the recently launched RFID pilot projects of the METRO Group. Technology-neutral legislation in this context means legislation that applies to all technologies and not to one in particular, whereas technology-specific regulation such as RFID-specific regulation specifically applies to the RFID technology only.

The analysis in this chapter is structured in a layered fashion. It starts with the regional tier (section 5.2) followed by the national (section 5.3), transnational (section 5.4), international (section 5.5), then goes back to the local tier of the RFID pilot projects of the MGFSI (section 5.6), and ends with the conclusion (section 5.7).

5.2 Regional tier of the governance regime – Nordrhein-Westfalen (Q2-Q4)

This section explores the regional tier of the emerging governance regime for consumer privacy protection in the embodiment of the Nordrhein-Westfalen. Section 5.2.1 explores the established technology-neutral consumer privacy legislation in Nordrhein-Westfalen. Subsequently, section 5.2.2 explores the role of Nordrhein-Westfalen in the development of RFID-specific regulation against the backdrop of the technology-neutral consumer privacy legislation.

5.2.1 Established technology-neutral consumer privacy legislation in Nordrhein-Westfalen⁶⁴

Nordrhein-Westfalen (NRW) is the biggest out of 16 federal states of the Federal Republic of Germany. The Nordrhein-Westfalen State Government enjoys considerable sovereignty and is responsible for making its own legislations and regulations. Nevertheless, the Federal Republic of Germany participates in the transnational context of the European Union (EU). As a result, EU legislations and regulations pass down to the federal tier and to the state tier and hence to Nordrhein-Westfalen.

In this study, the relevant consumer privacy legislation from the European tier is the technology-neutral ‘Data Protection Directive (95/46/EC)’, for the protection of individuals with regard to the processing of personal data and the free movement of such data of 24 October 1995. On the national tier in Germany, the technology-neutral ‘Federal Data Protection Act’ for the protection of personal data implements the ‘Data Protection Directive’. The ‘Federal Data Protection Act’ is in German called the ‘Bundesdatenschutzgesetz (BDSG)’ of 18 May 2001 and last amended on 5 February 2009. On the regional tier in Nordrhein-Westfalen, the technology-neutral ‘Data Protection Act NRW’ for the protection of personal data implements the ‘Data Protection Directive’. The ‘Data Protection Act NRW’ in German is called the ‘Datenschutzgesetz Nordrhein-Westfalen (DSG NRW), Gesetz zum Schutz personenbezogener Daten’ of 9 June 2000 and last amended on 29 April 2003.

The Nordrhein-Westfalen Commissioner for Data Protection and Freedom of Information⁶⁵, Regional Data Protection Commissioner for short, is the public data protection supervisory authority in Nordrhein-Westfalen. Since 1996, Ms Bettina Sokol has been the Data Protection Commissioner. Ms Sokol and her staff are responsible for monitoring and supervising that the data protection legislations are complied with in Nordrhein-Westfalen. The data protection legislation consists of both the state and federal data protection acts and data protection regulations governing specific areas. These legislations apply to the public sector of governmental institutions, other public organizations such as schools and hospitals, and the private sector of business enterprises.

In Germany, the data protection legislation governing *business enterprises* are laid down in the ‘Federal Data Protection Act’. In essence, companies are allowed to process personal data when, legal provisions permit it, or the person in question gave his/her consent. In addition, data protection regulation contained in special laws meant for specific areas take precedence over the general ‘Federal Data Protection Act’. Relevant for this study, a specific law that is meant for governing a specific area is the ‘Telecommunications Act’. The ‘Telecommunication Act’ implements the European tier ‘ePrivacy Directive (2002/58/EC)’ of 12 July 2002. Although still technology-neutral, the ePrivacy Directive concerns with the

⁶⁴ This section is a synthesis based upon: Interviews, Holland-Letz (2006); EC-DPD, 2009; LDI-NRW, 2009.

⁶⁵ For more information about the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI-NRW) consult: <https://www.ldi.nrw.de/>.

processing of personal data and the protection of privacy in the electronic communications sector. In German the 'Telecommunication Act' is called the 'Telekommunikationsgesetz (TKG)' of 22 June 2004.

In Germany, the data protection legislation governing the *public sector* that applies to the state are laid down in the data protection legislation of the particular state; in Nordrhein-Westfalen the 'Data Protection Act NRW'. Legislation for federal public institutions is laid down in the 'Federal Data Protection Act'. In essence, the same applies as for the private sector, the processing of personal data is allowed when, legal provision permit it, or the person in question gave his/her consent. In addition, in the public sector also applies that data protection regulation contained in special laws that are meant for a specific area take precedence over the general 'Federal Data Protection Act'.

Well, what have these data protection legislations to do with RFID pilot projects of the MGFSI? Well, the MGFSI deploys its RFID applications on consumer products (CPILT) in the Future Store located in Nordrhein-Westfalen. RFID is Information Technology (IT) and therefore is subjected to data protection legislation concerning processing of personal data and the protection of privacy of natural persons. Consequently, the Regional Data Protection Commissioner as the data protection supervising authority has the responsibility to monitor and supervise whether the MGFSI complies with the applicable data protection regulation. For business enterprises in the private sector, these are laid down in the 'Federal Data Protection Act' and the 'Telecommunications Act'.

5.2.2 The role of Nordrhein-Westfalen in the emerging RFID-specific consumer privacy regulation⁶⁶

After the consumer privacy controversy of METRO 1 in the Future Store in 2004, several developments took place in Nordrhein-Westfalen regarding consumer privacy and the RFID pilot projects of the MGFSI. In other word, developments regarding the compliance of the MGFSI with established technology-neutral data protection legislations and newly developed RFID-specific regulation.

The Regional Data Protection Commissioner interacts directly with the MGFSI as it monitors, supervises and consults with the MGFSI. They make sure the MGFSI complies with the established data protection legislations in the data processing activities of their RFID pilot projects. As we shall see later on in this chapter, the EC addresses consumer privacy concerns in RFID enabled applications. The EC proposed a Privacy Impact Assessment (PIA) in the draft version of their 'RFID Privacy, Data Protection and Security Recommendation' of February 2008. This is not official RFID-specific regulation in the EU yet. The MGFSI however voluntarily followed this advise and conducted a PIA of the their RFID pilot projects in the new Future Store in Toenisvorst (2008) and in the Galeria Kaufhof (2007) (see later this chapter). The results of the PIA were presented and approved of by the Regional Data Protection Commissioner.

The Regional Data Protection Commissioner works together with their umbrella organization on the national tier, the Federal Commissioner for Data Protection and Freedom of Information⁶⁷, Federal Data Protection Commissioner for short. In addition, the Regional Data Protection Commissioner keeps their fellow 15 Regional Data Protection Commissioners and the Federal Data Protection Commissioner up to date about the RFID

⁶⁶ This section is based upon a synthesis of the following sources: Holland-Letz (2006) and the interview with Brigitte Rittmann-Bauer (Consumer Center Nordrhein-Westfalen). Unfortunately, my insights in the regional tier of the emerging governance regime are somewhat thin. Besides that my limited resources the reason is that the regional tier is not as important for the development of RFID-specific regulations as the national, transnational and international tiers. Hence, I devoted my resources accordingly.

⁶⁷ For more information about the Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) consult: <http://www.bfdi.bund.de/>.

activities of the MGFSI in relation to data protection. All the Data Protection Commissioners engage in negotiations and discussions with each other and with other relevant organizations concerning data protection. These debates concern themselves with the established technology-neutral data protection legislations and the emerging RFID-specific regulations. As these take place on a national tier, they will be discussed in the next section.

Another organization that is relevant for the regional tier is the consumer organizations called Consumer Center Nordrhein-Westfalen⁶⁸, Regional Consumer Center for short. The Ministry of the Environment and Conservation, Agriculture and Consumer Protection of the German State of Nordrhein-Westfalen⁶⁹ is the main governmental body that supports the Regional Consumer Center. Nevertheless, the Regional Consumer Center as an NGO is able to autonomously safeguard consumer interests. The Regional Consumer Center investigates and studies what the MGFSI undertakes qua RFID applications on consumer products and what this means for consumer privacy. In addition, if any, the Regional Consumer Center collects consumer complaints regarding the RFID pilot projects of the MGFSI. In addition, the Regional Consumer Center educates, informs and advises consumers about new technologies such as RFID. The Regional Consumer Center also monitors whether data legislation and regulation from the national tier and transnational tier are complied with by the MGFSI in their RFID pilot projects. In protecting consumer interests, they work together with the Regional Data Protection Commissioner. Furthermore, the MGFSI invites the Regional Consumer Center for guided tours in their RFID pilot projects such as the Future Store to fully inform them about their RFID activities. Therefore, direct interaction between the Regional Consumer Center and the MGFSI takes place. The negotiations and discussions regarding the development of RFID-specific regulations for safeguarding consumer privacy take place on the national tier and transnational tier.

The umbrella organization the Federation of German Consumer Organizations⁷⁰, Federal Consumer Center for short, represents the voice of the German consumer on the national tier. The Federal Consumer Center consists of 16-consumer centers of the German federal states and 25 other consumer organizations. FoeBuD is not part of the Federation of German Consumer Organizations. The Federal Consumer Center and the associated network of organizations and their about eight million members provide a counterwelling force for industry and retailers such as the METRO Group. The Federal Consumer Center lobbies for favorable consumer policies by informing politicians and policy makers. They also see to it that consumer protection legislation is implemented and they provide advice for consumer. The Regional Consumer Center assists the Federal Consumer Center in formulating position statements on RFID that are used in the negotiations on the national tier and transnational tier. Next section will elaborate on the negotiations that take place on the national tier.

The Nordrhein-Westfalen State Government perceives RFID to have potential for the economical development of Nordrhein-Westfalen. As a result, it stimulates RFID innovations between industry and academia.⁷¹ The Regional Consumer Center and the Regional Data Protection Commissioner therefore interact with the Nordrhein-Westfalen State Government regarding warranting consumer interest of RFID.

In figure 19 below you will find the regional tier arena of the emerging governance regime for consumer privacy protection, fleshed out by Nordrhein-Westfalen. It shows how the MGFSI with their RFID pilot projects in the local tier arena is embedded in the data protection legislative and regulatory context of the regional tier arena of Nordrhein-Westfalen.

⁶⁸ For more information about the Verbraucherzentrale NRW (VZ-NRW) consult: <http://www.vz-nrw.de/>.

⁶⁹ For more information about the Ministerium für Umwelt und Naturschutz, Landwirtschaft und Verbraucherschutz des Landes Nordrhein-Westfalen (MUNLV) consult: <http://www.umwelt.nrw.de/>.

⁷⁰ For more information about the Verbraucherzentrale Bundesverband (VZ-BV) consult: <http://www.vzbv.de/>.

⁷¹ For more information about the NRW State Government and in particular regarding RFID consult: <http://www.media.nrw.de/media2/site/index.php?id=70>.

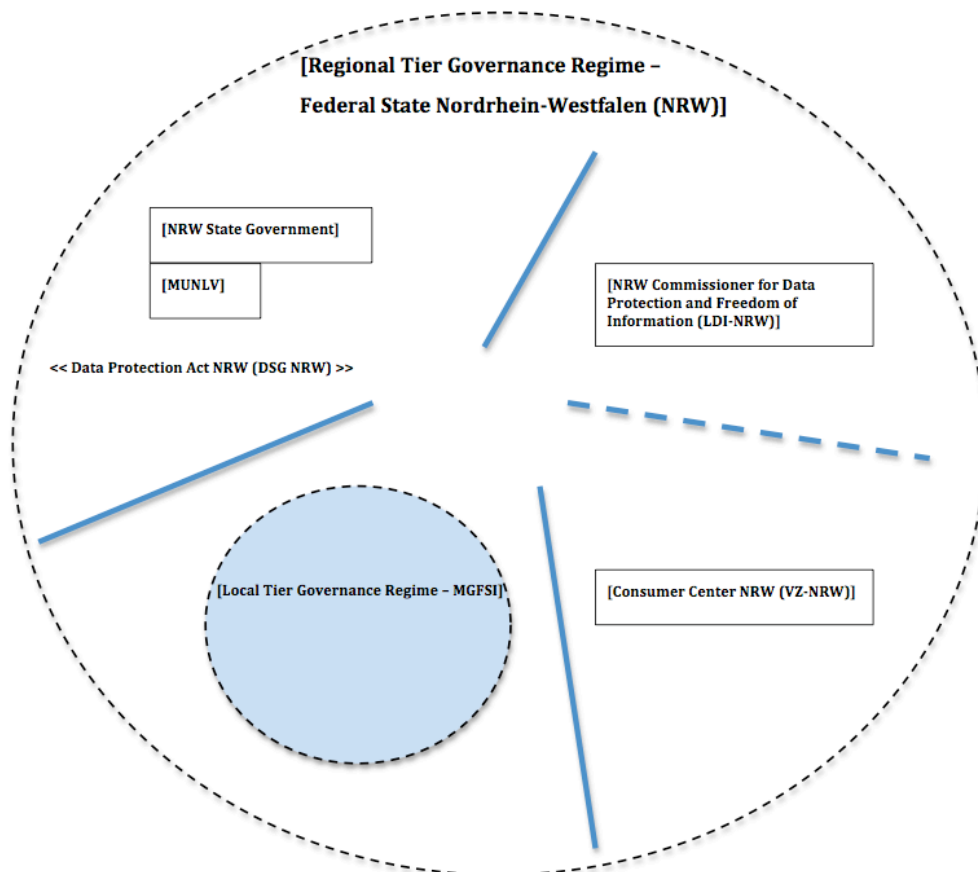


Figure 19 - Regional tier arena of the emerging governance regime for consumer privacy protection

5.2.3 Conclusion

This section discussed the links of the technology-neutral data protection legislation of the regional, national, and transnational tiers that run parallels with the multi-tier governmental institutions of Nordrhein-Westfalen, Germany, and the European Union. Furthermore, it discussed the relation of the Regional Consumer Center with the Federal Consumer Center, the Regional Data Protection Commissioner with the Federal Data Protection Commissioner, and these organizations with the MGFSI and each other. The Regional Consumer Center and the Regional Data Protection Commissioner closely monitor the RFID pioneering activities of the MGFSI. They perceive RFID on consumer products in a nuanced way. As long as the MGFSI complies with the applicable data protection legislations and no RFID misconduct regarding consumer privacy takes place, they do not perceive RFID applications as problematic. The regional tier is important as the Regional Data Protection Commissioner and the Regional Consumer Center keep their fellow regional and their national umbrella organizations abreast upon the RFID related developments of the MGFSI. Finally, the Regional Data Protection Commissioner and the Regional Consumer Center interact with the Nordrhein-Westfalen State Government in matters regarding safeguarding consumer interest in relation to RFID.

The formulation of RFID-specific regulation takes place on the national and transnational tiers and will be discussed in the next sections.

5.3 National tier of the governance regime – Federal Republic of Germany (Q2-Q4)

This section explores the national tier of the emerging governance regime for consumer privacy protection in the embodiment of the Federal Republic of Germany. Section 5.3.1 explores the established technology-neutral consumer privacy legislation in Germany. Subsequently, section 5.3.2 explores the RFID-specific regulation that is developed against the backdrop of the technology-neutral consumer privacy legislation.

5.3.1 Established technology-neutral consumer privacy legislation in Germany

Last section explained the interrelationships of the European tier, federal tier and state tier concerning technology-neutral data protection legislation. On the federal tier, the ‘Federal Data Protection Act’ implements the ‘Data Protection Directive’. The ‘Telecommunications Act’ implements the ‘ePrivacy Directive’. The last amendment to the ‘Telecommunications Act’ implements the ‘Data Retention Directive (2006/24/EC)’ of 15 March 2006. The ‘Data Retention Directive’ was adopted after the terrorist attacks in Madrid and London. On the EU tier, the ‘Data Retention Directive’ corresponds with the ‘Data Protection Directive’ and is an amendment of the ‘ePrivacy Directive’. The ‘Data Retention Directive’ not surprisingly concerns itself with the ‘retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.’

On the state tier of Nordrhein-Westfalen, the ‘Data Protection Act NRW’ implements the EU ‘Data Protection Directive’. Nevertheless, the ‘Data Protection Act NRW’ applies to the public sector of governmental institutions and other public organizations in Nordrhein-Westfalen. The ‘Federal Data Protection Act’ and the ‘Telecommunication Act’ apply to the private sector of business enterprises in Germany. Consequently, these two are relevant for the RFID applications of the MGFSI and the application of RFID on consumer products in the German retail sector in general.

The next section concerns itself with the emerging RFID-specific regulations that are developed against the backdrop of the ‘Federal Data Protection Act’ and the ‘Telecommunication Act’. The RFID-specific regulation builds upon the international EPC industry self-regulation, the industry code of conduct in the embodiment of the ‘EPCglobal Guidelines on EPC for Consumer Products’ as discussed in section 4.5 of the previous chapter.

5.3.2 Emerging RFID-specific consumer privacy regulation in Germany

5.3.2.1 Recommendation on RFID by the Düsseldorf Kreis

The Federal Data Protection Commissioner and the 16 regional Data Protection Commissioners make sure that the ‘Federal Data Protection Act’ and the ‘Telecommunication Act’ are abided in Germany.⁷² The discussions regarding the data protection regulation applicable to the private sector of business enterprises takes place in conferences organized by the ‘Düsseldorf Kreis’. This is an informal union of the Data Protection Supervisory Authorities for reflecting and discussing the established data protection regulations applicable to the private sector.⁷³ The ‘Düsseldorf Kreis’, published a recommendation on the

⁷² For an overview of the data protection supervisory authorities in Germany for the public sector consult: https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Datenschutzbeauftragte/Datenschutzbeauftragte.php.

⁷³ For an overview of the data protection supervisory authorities in Germany for the private sector consult: https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Aufsichtsbehoerden/Aufsichtsbehoerden.php.

application of RFID in the private sector after their conference in Bremen of 8/9 November 2006 (Kreis, 2006).

In short, the recommendation pleads for a ‘responsible data protection conform use’ of the RFID technology in the retail and the service sector. When being implemented, the recommendation allows for the development and application of RFID in the retail and the service sector in accord with existing data protection legislation. The recommendation recognized that RFID tags may not store personal data, but can become personal data when the data on the tags is coupled with personal data prior stored in information systems and databases. Consequently, consumer profiles can be established, especially when in the future all kinds of items in our daily life, such as groceries and apparel, may be tagged with RFID. Therefore, it is important that consumers remain in control over their personal data in RFID enabled applications (‘informationelle Selbstbestimmung’).

The ‘Recommendation on RFID’ calls for comprehensive, binding and testable RFID self-regulation in the retail and the service sector. This as the current data protection legislations are not adequate to incorporate the potential data protection risks associated with RFID. According to the recommendation, self-regulation and thus RFID enabled applications in the private sector should be bound to the following rules. Firstly, RFID applications should be transparent and consumers should be informed about how RFID works and when personal data is stored (‘Transparenz / Benachrichtigungspflicht’). Secondly, it should be clear to the consumer when RFID tags, readers and background systems are used (‘Kennzeichnungspflicht’). Thirdly, consumers should have the ability to deactivate the RFID tags after purchase (‘Deaktivierung’). Fourthly, data generated by RFID should be protected from misuse by third parties (‘Datensicherheit’). Finally, it is not allowed to employ RFID for building consumer profiles without consumers’ consent (‘Keine heimliche Profilbildung’).

The ‘Recommendation on RFID’ by the ‘Düsseldorfer Kreis’ marks the call from the Data Protection Authorities in Germany for RFID-specific regulation on the national tier and in particular self-regulation of retail and industry. As next section will show, there was an industry-self regulation initiative for a code of conduct that took place on the national tier between private and public stakeholders.

5.3.2.2 Industry self-regulation initiative for a code of conduct for EPC in retail

In the period between 2005 and 2008, on national tier in Germany a three-staged voluntary self-regulation initiative took place. These consisted of fora for dialog and negotiations by private and public stakeholders regarding a national code of conduct for the EPC industry in retail for warranting consumer privacy. The negotiations in the self-regulation initiative build upon the prior published EPC industry self-regulation ‘EPCglobal Guidelines for EPC on Consumer Products’ from 1 January 2005 and the ‘Recommendation on RFID’ by the ‘Düsseldorfer Kreis’ of 8/9 November 2006. The self-regulation initiative was not open to the public and hence did not produce any publicly available documents. Nevertheless, I was able to reconstruct (based upon interviews and email correspondences)⁷⁴ the following processes and outcomes of the three-staged self-regulation initiative.

⁷⁴ This section is a synthesis based upon: the *interviews* with Rena Tangens (FoeBuD), Katja Mrowka and Christian Thorun (Federation of German Consumer Organizations), Alexander Dix (Berlin Commissioner for Data Protection and Freedom of Information), Simon Japs (Informationsforum RFID), Brigitte Rittmann-Bauer (Consumer Centre Nordrhein-Westfalen) and *email correspondence* with Simon Japs (Informationsforum RFID), Christian Thorun (Federation of German Consumer Organizations), Axel Toenjes (Berlin Commissioner for Data Protection and Freedom of Information), Sandra Hohenecker (GS1-Germany), and Dirk Bungard (Federal Commissioner for Data Protection and Freedom of Information).

A three-staged industry self-regulation initiative

The *first stage* of the self-regulation negotiations was initiated, moderated, and took place at the Federal Ministry of Economics and Technology (BMWi)⁷⁵ in 2005. The BMWi is the governmental institution in Germany that promotes innovative technologies such as RFID. They perceive RFID to have tremendous potential for stimulating retail and industry and hence the German economy and its competitiveness within a global market. Nevertheless, they realize that for consumers to accept RFID, especially in the retail sector, adequate consumer protection regulations need to be in place (BMWi, 2006; BMWi, 2007). As a result, the BMWi played a moderating role in the forum in which the following contesting private and public stakeholders participated: FoeBuD, German Association for Data Protection (DVD)⁷⁶, GS1-Germany (representative of EPCglobal in Germany)⁷⁷, METRO Group, Federal Consumer Center, Federal Data Protection Commissioner, Informationsforum RFID⁷⁸, Federal Ministry of the Interior (BMI)⁷⁹, Federal Office for Information Security (BSI)⁸⁰, IBM-Germany⁸¹, German Association for Information Technology Telecommunications and New Media (BITKOM)⁸², and the RFID task force of the European Institute for Computer Anti-Virus Research (EICAR).⁸³ In 2006, after a few meetings the Informationsforum RFID stopped participating in the forum because of FoeBuD's anti-RFID position that allowed no room for negotiation. A couple of months later FoeBuD stopped participating in the forum as well, as for FoeBuD too there was no room to negotiate as they held on to their anti-RFID position. Half way through 2006, the negotiation in the forum deadlocked, because the remaining participants could not reach consensus.

In the *second stage* of the self-regulation initiative the dialog and negotiations resumed in a smaller forum at the Informationsforum RFID, being moderator this time, at the end of 2006. Participants in the forum for dialog and negotiations were GS1-Germany, METRO Group, the Federal Consumer Center and the Federal Data Protection Commissioner. FoeBuD and the BMWi did not participate in this smaller forum. In 2007, this second forum came close to an agreement, but had to stop prematurely before a final agreement could be reached. The reason for this was that the member organizations of the Federal Consumer Center did not want to sign an industry self-regulation, because of disappointing experiences in the past. This result not only led to disappointment with the EPC industry represented by the Informationsforum RFID, the METRO Group and GS1 Germany, but also with the consumer interest protectors, the Federal Consumer Center and the Federal Data Protection Commissioner.

The *third stage* of the industry self-regulation initiative is still in progress, but is suspended since February 2008. Participants in this forum are the Informationsforum RFID, GS1-Germany, METRO Group, Federal Data Protection Commissioner and the Federal Ministry of Food, Agriculture and Consumer Protection (BMELV).⁸⁴ The involved stakeholders are waiting for the final version of the EC 'RFID Privacy, Data Protection and Security Recommendation'.

⁷⁵ For more information on the Bundesministerium für Wirtschaft und Technologie (BMWi) consult: <http://www.bmwi.de/>.

⁷⁶ For more information about the Deutsche Vereinigung für Datenschutz (DVD) consult: <http://www.datenschutzverein.de/>.

⁷⁷ For more information about GS1-Germany consult: <http://www.gs1-germany.de/>.

⁷⁸ For more information about the Informationsforum RFID consult: <http://www.info-rfid.de/>.

⁷⁹ For more information about the Bundesministerium des Innern (BMI) consult: <http://www.bmi.bund.de/>.

⁸⁰ For more information about Bundesamt für Sicherheit in der Informationstechnik (BSI) consult: <http://www.bsi.de/>.

⁸¹ For more information about IBM Germany consult: <http://www.ibm.com/de/de/>.

⁸² For more information about German Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM): consult: <http://www.bitkom.org/>.

⁸³ For more information about RFID task force of the European Institute for Computer Anti-Virus Research (EICAR) consult: <http://www.eicar.org/>.

⁸⁴ For more information about the Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) consult: <http://www.bmelv.de/>.

Contesting stakeholders with opposing perspectives

In the negotiations of the industry self-regulation initiative, the contesting stakeholders have different perspectives. Nevertheless, they agree that the economical benefits for the German industry and hence the economy are the main incentives for employing RFID. Furthermore, as currently RFID is primarily employed in logistics, item-level tagging could be the next major step in the RFID evolution, although estimated 7 to 10 years away. Costs, together with consumer acceptance are perceived of as the pivotal determining factors for the further rollout of RFID on consumer products.

FoeBuD, which played a key role in revealing the METRO 1 consumer privacy controversy, put consumer privacy on top of the consumer acceptance agenda for RFID. As a result, the established consumer interest organizations, such as the Federal Consumer Center, the Federal Data Protection Commissioner and the other Data Protection Authorities started looking at RFID and its threats for consumer privacy. For the EPC industry and especially the METRO Group, the METRO 1 consumer privacy controversy was a wake-up call too. In April 2005, the EPC industry established a dialog platform called the Informationsforum RFID, to stimulate the public debate about RFID between consumers, industry and politics. The METRO Group is one of its founders and is represented in its executive board. In addition, GS1-Germany, the representative of EPCglobal in Germany, is one of its primary sponsors. Other large industrial organizations that take part in the Informationsforum RFID are: Deutsche Post World Net (DHL), Henkel Germany⁸⁵, Hewlett Packard Germany⁸⁶, IBM, Oracle Germany⁸⁷, Siemens Germany⁸⁸, T-Systems⁸⁹, Volkswagen⁹⁰, BITKOM, Federal Logistics Organizations (BVL)⁹¹, and the Fraunhofer-Institute for Material Flow and Logistics (IML).⁹² These industrial organizations clearly have an economical interest in RFID. Therefore, it does not come as a surprise that the consumer interest organizations, the Federal Consumer Center, the Federal Data Protection Commissioner, and FoeBuD, perceive the Informationsforum RFID as a political lobby organization for the RFID industry in Germany.

The mission of the Informationsforum RFID seems to prevent the development of strict RFID-specific regulation by the German Government. They perceive the current data protection regulation to suffice for warranting consumer privacy in RFID enabled applications. On the other hand, the Federal Consumer Center, the Federal Data Protection Commissioner, and the other consumer interest organizations form a counter movement and lobby for the protection of consumer interests. They are advocates of preventive RFID-specific regulation and preferably legislation. Although RFID is still premature, they are afraid that the market will grow fast and that it would be too late to make RFID-specific legislations. Nevertheless, with the exception of FoeBuD, they perceive strict RFID-specific legislation to be harmful for the development of RFID as well. Therefore, to balance the consumer privacy risks and the consumer benefits of RFID, they are in favor of strict industry self-regulation. Potential perceived consumer benefits of RFID are: lower prices for consumer products, reduced out of stocks, increased brand authentication, better best-before-date management, more convenient product recall, and additional services such as information terminals in stores. Because of their balanced perspectives, the Federal Consumer Center and the Federal Data Protection Commissioner are able to participate in the negotiations with the EPC industry, whereas FoeBuD because of its radical anti-RFID position is not.

⁸⁵ For more information about Henkel Germany consult: <http://www.henkel.de/index.htm>.

⁸⁶ For more information about Hewlett-Packard Germany consult: www.hp.com/de.

⁸⁷ For more information about Oracle Germany consult: www.oracle.de.

⁸⁸ For more information about Siemens Germany consult: www.siemens.de/rfid.

⁸⁹ For more information about T-Systems consult: www.t-systems.de.

⁹⁰ For more information about Volkswagen consult: www.volkswagen-ag.de.

⁹¹ For more information about Bundesvereinigung Logistik (BVL) consult: www.bvl.de.

⁹² For more information about the Fraunhofer-Institut für Materialfluss und Logistik (IML) consult: <http://www.iml.fraunhofer.de/1327.html>.

Figure 20 below depicts the national tier arena of the emerging governance regime for consumer privacy protection, in relation to the regional tier arena of Nordrhein-Westfalen and the local tier arena of the MGFSI. In figure 20, the upper left corner depicts the governmental institutions that predominantly have a moderating role. The consumer and data protection advocate institutions inhabit the upper right corner. The EPC industry and retail institutions inhabit the lower left corner. Finally, the Fraunhofer-Institute for Material Flow and Logistics (IML), as a pivotal RFID research institute in Germany, inhabits the lower right corner.

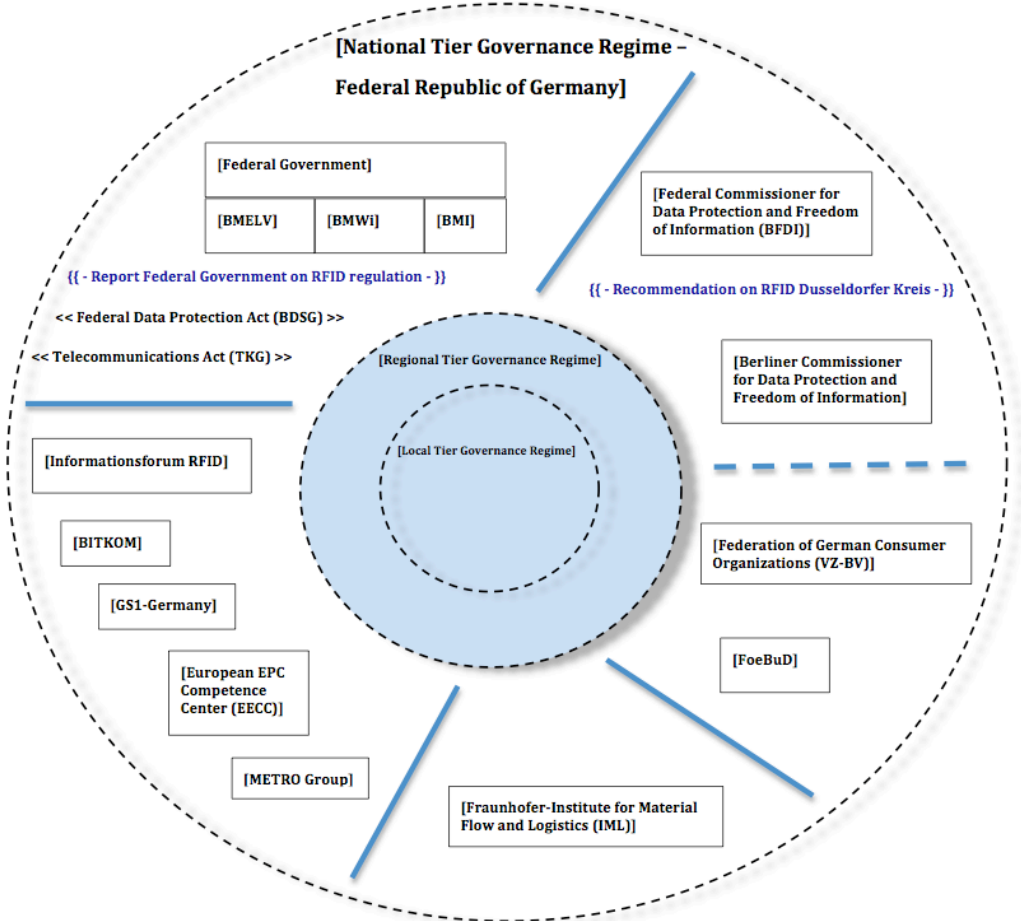


Figure 20 - National tier arena of the emerging governance regime for consumer privacy protection

The main issue is ‘opt-in vs. opt-out’

Since 2005, the contesting stakeholders in the industry self-regulation initiative came closer together and reached consensus on a whole range of issues. These issues were: transparency of RFID readers and tags indicated by logos, stimulating consumer awareness of RFID, the development and application of Privacy Enhancing Technologies (PET) to enhance consumer privacy, equal treatment of customers who use RFID and those who do not, and the keeping of cash check outs for anonymous shopping. Several of these agreements are already codified in the ‘EPCglobal Guidelines on EPC for Consumer Products’ and the ‘Recommendation on RFID’ by the ‘Düsseldorfer Kreis’.

Deactivation beyond the point of sale was the crucial element the negotiators could not find consensus on and hence the negotiations deadlocked. The core issue that caused the deadlock is the ‘opt-in vs. opt-out’ issue. ‘Opt-in’ means that consumer products tagged with RFID tags in retail need to be deactivated at checkout, unless consumers indicate otherwise. On the other hand, ‘opt-out’ means that consumers need to indicate at the checkout that they want the RFID tags to be deactivated, or consumers should have the ability to conveniently deactivate the RFID tags by themselves.

The ‘opt-out’ is already part of the ‘EPCglobal Guidelines on EPC for Consumer Products’ and the ‘Recommendation on RFID’ by the ‘Düsseldorfer Kreis’. The consumer and data protection organizations, the Federal Consumer Center and the Federal Data Protection Commissioner want to take it a step further and want ‘opt-in’ as the standard in the retail sector. They will not take any risks concerning a potential consumer privacy invasion by RFID beyond the point of sale. The METRO Group, GS1-Germany, and the Informationsforum RFID favor the ‘opt-out’ option. The EPC industry is not in favor of ‘opt-in’ because it would rule out any potential post purchase benefits of RFID in the future. More importantly, ‘opt in’ would entail the costly installation of RFID deactivators at every point of sale in retail. As the RFID is still premature and not widely used on item-level, this would make a bad business case for the EPC industry.

As a result, the dispute could not be resolved and the negotiations were suspended. The ‘hot potato’ of ‘opt-in vs. opt-out’ together with the question whether RFID-specific legislations are needed, was passed on to the political arenas of the Federal Government and European Commission (EC).

The Federal Government advocates industry self-regulation

On 23 of January 2008, the German Parliament⁹³ together with Federal Ministry of the Interior (BMI) published a report on the activities and plans for possible legislative action in relation to the data protection effects of the RFID technology (Bundestag, 2008). This report of the German Government explored three options: an amendment of the ‘Federal Data Protection Act’ to incorporate RFID-specific regulation, separate RFID-specific legislation, and industry self-regulation. Because the RFID technology is still immature and RFID applications for consumer products are not pervasively present, in combination with that the EC is about to release the final version of their ‘RFID Privacy, Data Protection and Security Recommendation’, made the German Government advocate an industry self-regulation for RFID. Since the industry-self-regulation initiative is suspended, all the eyes are directed towards the EC.

On the one hand, RFID-specific legislation can be considered advantageous, because it creates clarity for all the involved stakeholders. On the other hand, it can be considered disadvantageous, as strict legislation can hamper the innovation potential of RFID that is still in an experimental and embryonic stage. An industry self-regulation initiative in the form of a

⁹³ For more information about the Deutscher Bundestag consult: <http://www.bundestag.de/>.

code of conduct could be a workable middle way. It would provide regulation though being flexible at the same time. However, the weak spot of industry self-regulation is that it is its flexibility as it is easily changed. In addition, industry self-regulation lacks accountability and any mechanism for legal sanctions when it is violated.

In the three-staged industry self-regulation initiative a temporary code of conduct of about 3-4 years was discussed. In that way, RFID could mature and it would become clear whether it would be technically and economically feasible for item-level tagging. Then after 3-4 years, the discussion of 'opt-in vs. opt-out' would be more practical. In addition, a monitoring board, consisting 'fifty-fifty' out EPC industry and consumer protection authorities, would be installed to monitor the proceedings. Furthermore, within the context of consumer acceptance of RFID and industry self-regulation, the press functions as a powerful sanction mechanism. It is not in the interest of the EPC industry to violate consumer's trust, by receiving bad press when they would violate a code of conduct. This would not only be bad for their business but also impede upon consumer acceptance of RFID. Contrarily, good press and Public Relations (PR) are beneficial for their business and the acceptance of the EPC standard in retail. Consequently, creating a powerful incentive for the EPC industry to keep an agreed upon code of conduct.

In conclusion, industry self-regulation, when being agreed upon by all the relevant stakeholders, definitely has the potential to mitigate negative aspects for consumer privacy, while allowing experimentation with the constructive aspects of RFID.

The European Commission as the highest authority

The EC has to make the tough decision concerning the 'opt-in vs. opt-out' issue. All the stakeholders in the self-regulation initiative forum, incl. the German Government, are waiting for the EC to publish the final version of their 'RFID Privacy, Data Protection and Security Recommendation'. Currently, the final version of the EC 'RFID Privacy, Data Protection and Security Recommendation' is going through intra-service consultation and is expected to be published in Spring 2009 (more about this in the discussion chapter).

After the publication of the final version of the EC 'RFID Privacy, Data Protection and Security Recommendation', the negotiations of the third stage of the German industry self-regulation forum will resume. Nevertheless, there is no guarantee that the industry self-regulation might actually work out and yield the desired code of conduct for the German EPC industry. In case of a deadlock again, the stakeholders expect the German Government not to proceed to RFID-specific legislation for at least 1.5 years, as there will be elections in Germany next year.

5.3.3 Conclusion

This section showed that the technology-neutral data protection legislation of the national tier is interwoven with the regional tier and the transnational tier. The RFID-specific regulations on the national tier and on the transnational tier are interwoven as well. The RFID-specific regulations that emerged on the national tier were the ‘Recommendation on RFID’ by the ‘Düsseldorfer Kreis’ and the negotiations of private and public stakeholders in a three-staged self-regulation initiative for a code of conduct for the German EPC industry. The negotiations of the three-staged self-regulation initiative built upon the ‘EPCglobal Guidelines on EPC for Consumer Products’ and the ‘Recommendation on RFID’ by the ‘Düsseldorfer Kreis’. These negotiations deadlocked on the ‘opt-in vs. opt-out’ issue. The involved contesting private and public stakeholders and the German Government are now waiting for the final EC ‘RFID Privacy, Data Protection and Security Recommendation’ that has to provide the answer to the ‘opt-in vs. opt-out’ dispute. Table 9 below provides a comprehensive overview of the RFID-specific regulatory outcomes, processes, and involved institutions as discussed in this section. The next section will elaborate on the transnational tier of the EU.

Year	Outcomes	Processes	Institutions/Organizations	Interpretation
2005	- Informationsforum RFID	- EPC industry establishes the Informationsforum RFID to stimulate a positive public debate about RFID between consumers, industry, and politics. - Start first stage of the industry self-regulation initiative for a code of conduct for the EPC industry in retail. Dialog and negotiations between contesting private and public stakeholders under the supervision of the German Government	- METRO Group, DHL, Henkel, HP, IBM, Oracle, Siemens, T-Systems, Volkswagen, BITKOM, BVL, IML - BMWi (moderator), FoeBuD, DVD, GS1-Gemany, METRO Group, Informationsforum RFID, Federal Consumer Center, Federal Data Protection Commissioner, BMI, BSI, IBM-Gemany, BITKOM, EICAR	- Industry installs a public RFID lobby organization - Birth of discussing RFID-specific regulation in addition to established technology-neutral data protection legislation
2006	- Deadlock first stage of the industry self-regulation initiative - 'Recommendation on RFID' by the 'Düsseldorfer Kreis'	- Stop first stage industry-self regulation initiative, FoeBuD and Informationsforum RFID stepped out and negotiations deadlocked - Highest Data Protection Authorities in Germany consider RFID as a threat to data protection in the private sector - Start second stage of the industry self-regulation initiative for a code of conduct for the EPC industry in retail, this time in a smaller forum	- BMWi (moderator), FoeBuD, DVD, GS1-Gemany, METRO Group, Informationsforum RFID, Federal Consumer Center, Federal Data Protection Commissioner BMI, BSI, IBM-Gemany, BITKOM, EICAR - Highest Data Protection Authorities for the private sector in Germany - Informationsforum RFID (moderator), Federal Consumer Center, GS1-Gemany, METRO Group, Federal Data Protection Commissioner	- Difficult to dialog and negotiate with stakeholders that do not want to compromise - Data Protection authorities indicate that the established technology-neutral data protection legislations are not adequate to incorporate RFID - Negotiation resume with stakeholders that are willing to make concessions
2007	- Deadlock second stage of the industry self-regulation initiative	- Stop second stage of the industry self-regulation initiative for a code of conduct for the EPC industry in retail. Almost reached an agreement, but Federal Consumer Center member organizations bailed out - Start third stage of industry self-regulation initiative for a code of conduct for the EPC industry in retail	- Informationsforum RFID, Federal Consumer Center, GS1-Gemany, METRO Group, Federal Data Protection Commissioner - Informationsforum RFID, GS1-Gemany, METRO Group, Federal Data Protection Commissioner, BMELV	- The establishment of a code of conduct proves difficult - The remaining stakeholders decide to continue
2008	- Report German Government on RFID-specific legislation Third stage industry self-regulation put on hold	- German Parliament together with the BMI publishes a report on the possibilities for RFID-specific legislation. It recommends industry self-regulation and to wait for the EC 'RFID Privacy, Data Protection and Security Recommendation' - Third stage of the self-regulation initiative is set on hold, key issue 'opt-in vs. opt out' passed on to the German Government and the European Commission. Waiting for the EC 'RFID Privacy, Data Protection and Security Recommendation', then the negotiations will resume	- BMI, German Parliament - Informationsforum RFID, GS1-Gemany, METRO Group, Federal Data Protection Commissioner, BMELV	- German Government advocates an industry self-regulation and advises to wait for the EC 'RFID Privacy, Data Protection and Security Recommendation'. - The German Government and the stakeholders in the industry-self initiative forum are waiting for the EC to bring the solution on the 'op-in vs. opt-out' issue

Table 9 - Overview outcomes, processes, and involved institutions in the development of RFID-specific consumer privacy regulation in Germany between 2005-2008

5.4 Transnational tier of the governance regime – European Union (EU) (Q2-Q4)

This section explores the transnational tier of the emerging governance regime for consumer privacy protection in the embodiment of the EU. Section 5.4.1 explores the established technology-neutral consumer privacy legislation in the EU. Subsequently, section 5.4.2 explores the RFID-specific regulation that is developed against the backdrop of the technology-neutral consumer privacy legislation.

5.4.1 Established technology-neutral consumer privacy legislation in the EU

On the transnational EU tier, there are three interwoven technology-neutral data protection legislations in the form of Directives that are required to be implemented by the EU Member States in their national data protection legislations. In Germany, the ‘Federal Data Protection Act’ implements the ‘Data Protection Directive’. The ‘Telecommunications Act’ implements the ‘ePrivacy Directive’ supplemented by the ‘Data Retention Directive’.

An interesting observation is that the ‘Data Protection Directive’ is based upon the principles as laid down in the ‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ adopted by the Organization for Economic Co-operation and Development (OECD) on 23 September 1980 (OECD, 1980). Recall, these OECD Privacy Guidelines are the same as the consumer privacy and civil liberty NGOs referred to in their shared RFID Position Statement (see section 4.4.2 previous chapter). EPCglobal also employed the OECD Privacy Guidelines in constructing the EPCglobal Guidelines (see section 4.5.1 previous chapter). Hence, the OECD Privacy Guidelines are important guidelines that provide guidance for devising consumer privacy policy.

There is another interesting aspect of the ‘Data Protection Directive’. On 24 October 1995, simultaneously with its adoption conform Article 29 the ‘Article 29 Data Protection Working Party’ was instituted (EC-WP, 2009). The ‘Working Party’ is an independent advisory body that consists of the National Data Protection Commissioners of the EU Member States. For instance, ‘Peter Schar’, the Federal Data Protection Commissioner represents Germany in the ‘Working Party’.

The four main tasks of the ‘Working Party’ as specified in Article 30 of the ‘Data Protection Directive’ are as follows. Firstly, to provide expert opinion on data protection from the member state level to the EC. Secondly, to promote the uniform application of the ‘Data Protection Directive’ in the entire EU by means of active cooperation between data protection supervisory authorities. Thirdly, to update the EC about national measures that effects the rights and freedoms of natural persons qua processing of their personal data and privacy. Finally, formulate public recommendations and recommendations for the national level institutions on the matter of processing personal data and privacy, with the aim to protect persons within the EU. Not surprisingly therefore that the first recommendation on RFID-specific data regulation from the EU level came from the ‘Working Party’.

5.4.2 Emerging RFID-specific consumer privacy regulation in the EU

5.4.2.1 The European Commission (EC) and its RFID policy-making instruments

Parallel to the national tier in Germany, there are RFID-specific regulatory activities on the transnational tier in the EU. The department of the European Commission that develops RFID-specific regulation is the Directorate-General Information Society and Media (DG INFSO), led by Commissioner Viviane Redding (EC, 2009; EC-DG-INFSO, 2009). The DG INFSO has two interwoven responsibilities. On the one hand, it has the responsibility of devising policies for promoting, stimulating, and regulating innovations in ICTs in the EU (EC-DG-INFSO-Pol, 2009). On the other hand, it has the responsibility for the work on the ground, i.e. coordinating the activities that flow from these policies (EC-DG-INFSO-Act, 2009).

The activities of the DG INFSO concerning RFID take place within a much broader vision of the ‘Internet of Things’ (IoT) (EC-IoT, 2009; EC-RFID-Policy, 2009). The IoT is the vision that holds the seamless integration of the digital/virtual realm of the Internet with the physical realm of objects resulting in ‘interconnected objects having an active role in what might be called the Future Internet’ (EC & EPoSS, 2008: 6). The activities of the DG INFSO concerning devising RFID policies fall within the overall ‘i2010 – A European information society for growth and employment’ policy framework of the i2010 strategy that the EC launched in June 2005 (EC-i2010-strategy-doc, 2009). For a period of 5 years, the i2010 strategy aims at combining all the EU policies, initiatives, and actions related to innovations in ICTs that aim at contributing to the economic growth, job creation, and improving the personal quality of life within the EU. In turn, the i2010 strategy is part of the Lisbon strategy that was launched by the EC in 2005 following the Lisbon summit of March 2000. The Lisbon strategy aims at making Europe a dynamic knowledge-driven economy within a competitive global economy (EC-i2010-Lisbon, 2009).

The DG INFSO works together with the Directorate-General for Freedom Security and Justice (DG FSJ) in the development of RFID-specific regulation (EC-DG-FSJ, 2009). The DG INFSO together with the DG FSJ have several policy-making instruments at their disposal in the policy processes to formulate RFID-specific regulation for the EU. Their desired policy outcome is the EC ‘RFID Privacy, Data Protection and Security Recommendation’ to be implemented by the EU Member States.

Characteristic for the EC is that it adopts a deliberative approach by involving all the relevant stakeholders from the private sector (industry), public sector (government/other) and civil society (citizens) in public debates with the aim of finding consensus. In the public debates, the EC focuses on both the positive and the potential negative aspects of RFID. In doing so, the EC employs the following instrument. Firstly, the already discussed ‘Working Party’ that since its inception in 1995 performs ongoing scrutiny of established EU consumer privacy legislations and advises the EC accordingly. Secondly, since 2006, the DG INFSO has been organizing dedicated conferences, workshops, and symposia regarding the Internet of Things (IoT) and RFID in which they bring together all the relevant stakeholders (see EC-IoT, 2009 for an overview). Thirdly, since 2006, the DG INFSO has been holding Public Online Consultations on key RFID-related draft policy documents to involve the citizens of the EU and the other relevant private and public stakeholders. Stakeholders are able to comment on the documents generated by the EC staff and put up for Public Online Consultation. Consequently, the feedback on these documents is fed back in the policy-making process of the EC. Finally, since 2007, the RFID Expert Group that was established in 2007 advises the DG INFSO on matters related to RFID-specific regulations. In the RFID

Expert Group, key stakeholder from industry, government, and the civil society are represented (EC-Expert, 2009).

The activities of the DG INFSO on the research and development of ICTs take place within the context of the Seventh Research Framework Program (FP7, 2007-2013) and the Sixth Research Framework Program (FP6, 2002-2006) that are managed by the Directorate-General Research (DG Research) (EC-ICT-Research, 2009; EC-FP7, 2009; EC-FP6, 2009; EC-DG-Research, 2009). In January 2007, all EU RFID related R&D projects were subsumed under the Cluster of European RFID Projects (CERP). During the first year of operation, Gerd Wolfram from the METRO Group coordinated CERP (EC-CERP, 2009).

Germany is leading in Europe regarding the development and application of RFID. The German organizations, the ones described in the section on the national tier, play an important role in the policy-making process of the EC (see EC & BMWi, 2007; BMWi, 2008). The German organizations are represented well at EC conferences, workshops, and symposia. Besides, they comment on policy documents that are put up by the EC for Online Public Consultation.

See figure 21 below for an overview of the arena of the transnational tier of the emerging governance regime for consumer privacy protection in the EU. Additional to the EC and its policy instruments and hence indirectly the involved stakeholder organizations of the EU Member States, key organizations that play a role on the EU tier are the European Retail Round Table (ERRT)⁹⁴, The European Consumers' Organization (BEUC)⁹⁵, European Economic and Social Committee (EESC)⁹⁶ and European Data Protection Supervisor (EDPS).⁹⁷

⁹⁴ For more information about the European Retail Round Table (ERRT) consult: <http://www.errt.org/>.

⁹⁵ For more information about The European Consumers' Organization (BEUC) consult: <http://www.beuc.eu/>.

⁹⁶ For more information about the European Economic and Social Committee (EESC) consult: http://eesc.europa.eu/index_en.asp.

⁹⁷ For more information about the European Data Protection Supervisor (EDPS) consult: <http://www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=en>.

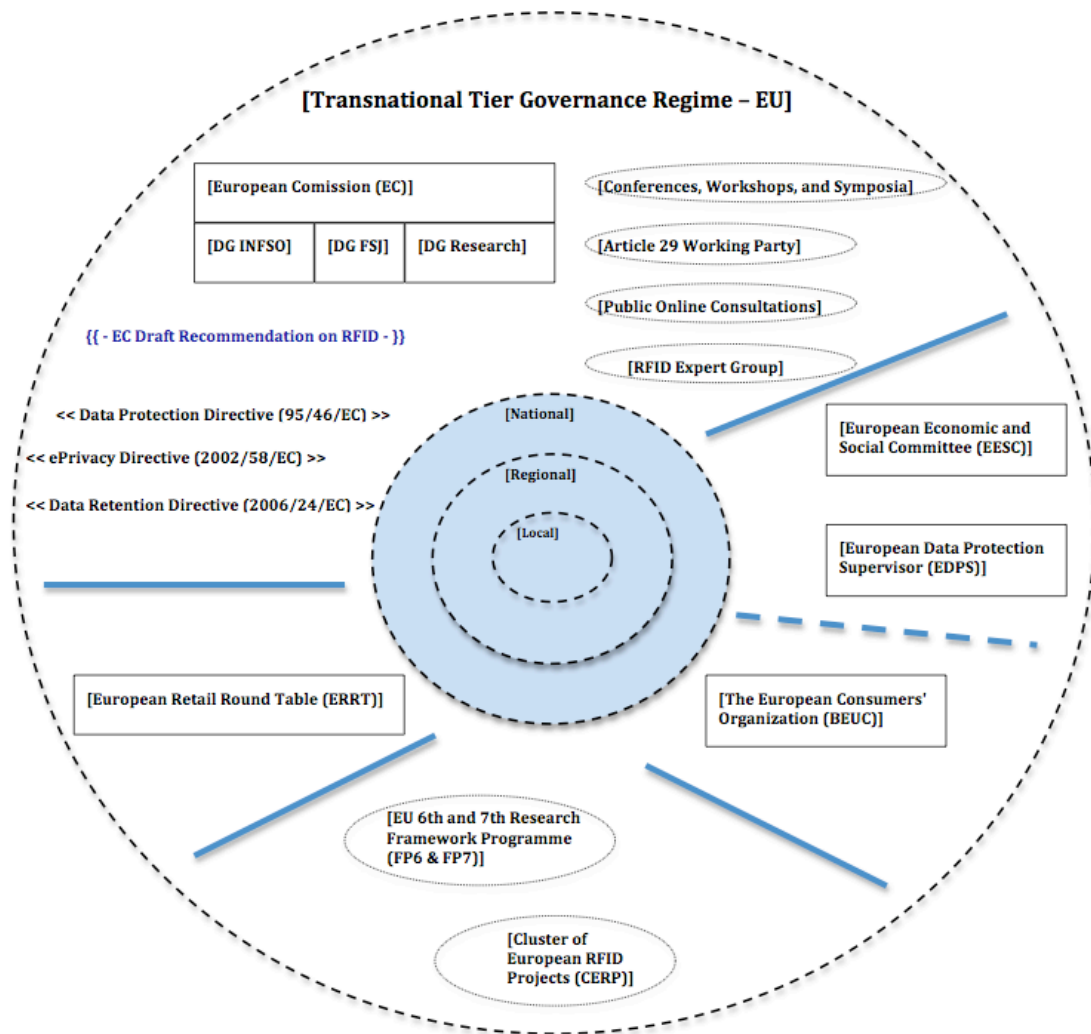


Figure 21 - Transnational tier arena of the emerging governance regime for consumer privacy protection

5.4.2.2 The EC ‘RFID Privacy, Data Protection and Security Recommendation’ on ‘opt-in vs. opt-out’⁹⁸

In the transnational arena, the policy-making processes for RFID-specific regulation takes place for the EU. Table 10 below provides a comprehensive overview of the key policy events and key policy outcomes in the policy-making processes orchestrated by the EC using their policy-instruments. The ‘Working Party’ initiated the need for RFID-specific regulation by publishing the first guidance on how the ‘Data Protection Directive’ should be applied to RFID enabled applications. What becomes clear when looking at table 10 is that since 2005 the EC RFID policy-making activities are converging to a *final* version of the ‘RFID Privacy, Data Protection and Security Recommendation’. In other words, an RFID-specific legal instrument to be transposed in data protection and consumer privacy legislation of the EU Member States.

The *draft* version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’ published on 21 February 2008, incorporates all the previously published and adopted policy documents and is refined in the successive policy-making process. The draft text recommends amongst other things: sector/application specific self-regulation (code of conduct), Privacy Impacts Assessment (PIA) of RFID applications, (built in privacy) privacy-by-design by developing Privacy Enhancing Technologies (PET), and consumer awareness raising of RFID.

Particularly interesting is article 7, devoted to RFID applications in retail. The Recommendation states that when RFID tags contain personal data or when the Privacy Impact Assessment (PIA) shows a likelihood of personal data being generated, RFID tags should be deactivated at the point-of-sale conform the ‘opt-in principle’. When no personal data is involved and the PIA shows no risk of personal data is generated, retailers should make available means for deactivating or removing the RFID tags if consumers want that, i.e. conform the ‘opt-out principle’. After three years, the EC will evaluate and when the state of the technology permits it, they want automated deactivation at every point of sale in retail conform the ‘opt-in principle’.

The aspiration of the EC for a full implementation of the ‘opt-in principle’ in retail, as stated in the draft version of the Recommendation, proves to be problematic for retailers. On the ‘Transatlantic RFID Workshop on Consumer Privacy and Data Security’ organized by the Federal Trade Commission (FTC) and the DG INFSO in Washington D.C. on September 23 2008, Paul Shekan from the EERR (representing European retailers incl. the METRO Group) drew a line in the sand. According to Shekan, when the final EC ‘RFID Privacy, Data Protection and Security Recommendation’ requires retailers to deactivate RFID tags at every point of sale, it would mean the end of item-level tagging in the European retail sector. The reason Shekan gives is that there are only a few items tagged and in the about 27.000 retail stores in Europe there are hundreds of thousands points of sale, which would require an enormous investment in RFID deactivators, something not economical feasible (FTC, 2008b).

The final version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’ therefore needs and probably will provide a decisive answer to the ‘opt-in vs. opt-out dispute’.

⁹⁸ This section is a synthesis based upon: EC-IoT, 2009; EC-RFID-Policy, 2009; EC-Memo, 2008, and my symposium attendance of the ‘Transatlantic RFID Workshop on Consumer Privacy and Data Security’ on 23 September 2008.

Year	Date	Outcome or Event	Description
2005	- 19 January 2005	- Article 29 Data Protection Working Party adopts 'Working document on the data protection issues related to RFID technology'	- This document (wp 105) provides guidance to RFID users on the application of basic principles in the EC Directives, particularly the Data protection Directive and the ePrivacy Directive. ⁹⁹
	- 1 June 2005	- EC adopts a Communication on the i2010 strategy	- The EC adopts Communication entitled: 'i2010 – A European Information Society for growth and employment' (COM (2005) 229 final) and with it launches the i2010 strategy. ¹⁰⁰
	- 25 September 2005	- Result Public Consultation on working document 105 (wp 105) of the Article 29 Data Protection Working Party	- The results (wp 111) of the Public Consultation on Article 29 Working Party Working Document 105 (wp 105) indicates different views among commentators regarding the definition of 'personal data', as well as the need for further guidance from the EC on privacy and data protection issues arising from RFID. ¹⁰¹
2006	- March 2006 – October 2006	- EC conducts a series of dedicated Workshops and a first Public Online Consultation	- EC conducts a series of dedicated Workshops and a first Public Consultation to build consensus on key issues associated with the development of RFID. ¹⁰²
2007	- 14 March 2007	- EC adopts an Communication on a RFID Policy Framework	- The EC adopts a Communication entitled: 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' (COM (2007) 96 final). ¹⁰³ This communication summarized the results of the previously held dedicated Workshops and the first Public Consultation. In addition, it indicates the work the public expects from the EC regarding privacy and data protection. In this Communication, the EC announced to work on a 'RFID Privacy, Data Protection and Security Recommendation' and the intention of setting up an 'RFID Expert Group'.
	- 20 June 2007	- Article 29 Data Protection Working Party adopts opinion on the concept of 'personal data'	- The Article 29 Working Party adopts an opinion (wp 136) on the concept of personal data (makes reference to RFID several times) that provides guidance on the concept of personal data in the Data Protection Directive (95/46/EC) and related Community legislation and its application in different situations. ¹⁰⁴
	- 28 June 2007	- EC adopts a Communication on the establishment of a RFID Expert Group	- The EC adopts an Communication and hence establishes an RFID Expert Group that would, amongst other things, advice the EC on elements to be included in an upcoming 'Recommendation on the implementation of privacy, data protection and information security principles in applications supported by RFID' (concept legal instrument). The meetings are not public hence yielding no publicly available documents. The communication in which the EC announces established RFID Expert Group: Communication entitled: 'Setting up an Expert Group on Radio Frequency Identification' (2007/467/EC). ¹⁰⁵

⁹⁹ This document is available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

¹⁰⁰ This documents is available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF>.

¹⁰¹ This document is available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf.

¹⁰² For an overview and the results of the dedicated workshops and the Public Consultation on RFID and the IoT consult: <http://www.iot-visitthefuture.eu/index.php?id=75>.

¹⁰³ This document is available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf.

¹⁰⁴ This document is available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

¹⁰⁵ For more information about the RFID Expert Group consult: <http://ec.europa.eu/transparency/regexpert/detail.cfm?ref=2040&l=all> or <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0467:EN:NOT>.

	- July 2007	- EC & BMWi adopt report entitled: 'European Policy Outlook RFID'	- This working document was initiated in the context of the German EU Presidency in 2007. The BMWi representing the German Government together with the EC DG INFSO organized a European Conference entitled: 'RFID: Towards the Internet of Things' in Berlin on 25th and 26th of June 2007. As a result the BMWi and the EC published the 'European Policy Outlook RFID' that was to form the basis for the EU RFID policy agenda from then on. The draft version served as a reference document in the conference. ¹⁰⁶
	- October 2007	- The European Economic and Social Committee (EESC) adopts an opinion on RFID	- The EESC adopts an opinion on RFID (2007/c 256/13). ¹⁰⁷ This opinion is incorporated in the draft EC 'RFID Privacy, Data Protection and Security Recommendation'.
	- December 2007	- The European Data Protection Supervisor (EDPS) adopts an opinion on the EC Communication of 2007 (COM (2007) 96 final)	- The EDPS adopts an opinion on the EC Communication of 2007 (2008/C 101/01). ¹⁰⁸ This opinion is incorporated in the draft EC 'RFID Privacy, Data Protection and Security Recommendation'.
2008	- 21 February 2008 – 25 April 2008	- Draft EC 'RFID Privacy, Data Protection and Security Recommendation' is put up for a Public Online Consultation	- The EC launched a Public Consultation on the draft text of the 'Commission Recommendation on the implementation of privacy, data protection, and information security principles in applications supported by radio-frequency identification.' ¹⁰⁹
	- September 2008	- German Government adopts reflection paper on the report entitled: 'European Policy Outlook RFID'	- The German Government (BMW) adopts a reflection paper entitled: 'From Berlin 2007 to Nice 2008 and Beyond: RFID – Internet of Things – Internet of the Future', a reflection on the report adopted in July 2007 entitled: 'European Policy Outlook RFID'. ¹¹⁰ Regarding consumer privacy, they welcome the EC 'RFID Privacy, Data Protection and Security Recommendation' in particular preventive Privacy Impact Assessment (PIA) of RFID enabled applications, and recommend self-regulation to solve the opt-in vs. opt-out issue in retail.
2009	- May 2009	- Anticipated: Final EC 'RFID Privacy, Data Protection and Security Recommendation'	- The final EC 'RFID Privacy, Data Protection and Security Recommendation' as a legal instrument for ensuring privacy and the protection of personal data in RFID enabled applications is pending. Most likely, the final Recommendation will provide a solution to the 'opt in vs. opt-out dispute'. The second Transatlantic Symposium on the Societal Benefits of RFID will be held on May 5th and 6th 2009 in Brussels will provide more clarity on the issue.

Table 10 - RFID-specific policy outcomes/events in the policy-making process orchestrated by the EC using their policy-making instruments between 2005 and 2009

¹⁰⁶ This document is available at: http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeucomission/European_Policy_Outlook_RFID.pdf.

¹⁰⁷ This document is available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:256:0066:0072:EN:PDF>.

¹⁰⁸ This document is available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:101:0001:0012:EN:PDF>.

¹⁰⁹ This document is available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/high_level_group/draft_recommendation_rfid.pdf.

¹¹⁰ This document is available at: http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeucomission/Reflections_on_European_Policy_Outlook_RFID.pdf.

5.4.3 Conclusion

In this section, we saw the emerging regulatory activities of the EC and its instruments for the development of RFID-specific consumer privacy regulations against the backdrop of the established technology-neutral consumer privacy legislations. Overall, the EC RFID-specific regulatory initiative can be characterized as proactive, anticipatory, deliberative, and top-down.

Since 2005, in the context of the i2010 Policy Framework, the Directorate-General Information Society and Media (DG INFSO) intensified its regulatory initiatives for RFID-specific regulations within their vision of the 'Internet of Thing' (IoT). In their regulatory processes the EC pursues to incorporate all the relevant stakeholders from industry, government, and the civil society. The key instruments the EC employs for the development of RFID-specific regulations are the 'Article 29 Data Protection Working Party', dedicated conferences, workshops, and symposia, an RFID Expert Group, and the R&D projects of RFID within Cluster European RFID Projects (CERP).

The EC aims at creating a comprehensive and uniform policy framework for data protection and consumer privacy for RFID among its Member States, i.e. a harmonized implemented policy framework among its Member States. This implies that all the EU Member States eventually implement comparable consumer privacy regulations that come from the transnational EU tier of the emerging governance regime. This would create a climate for consumer to accept and trust RFID and for industry to invest in consumer applications with RFID.

The major (dynamically-stable) RFID-specific regulatory outcome so far is the *draft* EC 'RFID Privacy, Data Protection and Security Recommendation' published on 21 February 2008. The draft builds upon the established technology-neutral data protection legislation. The *final* version of the EC 'RFID Privacy, Data Protection and Security Recommendation' is to provide the solutions the 'opt-in vs. opt-out' issue. In addition, it would also shed light upon the possible end of item-level tagging in the European retail sector. The EC expects to publish the final version of the EC 'RFID Privacy, Data Protection and Security Recommendation' in May 2009.

The activities of the EC increasingly take place in the transatlantic context with the US. Next section therefore will elaborate upon the international tier of the emerging governance regime for consumer privacy protection.

5.5 International tier of the governance regime – Transatlantic EU-US (Q2-Q4)

In the transatlantic relation between the EU and the US, there are dialogs and initiatives for harmonizing policy frameworks to lower potential trade barriers that hamper economic development. This section explores the RFID-specific regulatory dialogs and initiatives that take place in the transatlantic context.

In the previous chapter, we already saw two RFID-specific regulatory initiatives on the international tier. The first was a call for RFID-specific regulation in the embodiment of the shared RFID Position Statement published by consumer privacy and civil liberty NGOs in the US and EU on 20 November 2003. CASPIAN (US) and FoeBuD (EU) were the two leading NGOs in voicing consumer privacy concerns of RFID applications in the retail sector. Secondly, we saw the response from the EPC industry in terms of a voluntary self-regulation initiative that resulted in a code of conduct, to be complied with by all members of the EPC industry (EPC technology users and producers). EPC published its ‘EPCglobal Guidelines on EPC for Consumer Products’ on 1 January 2005. Figure 22 below depicts the International tier arena of the emerging governance regime for consumer privacy protection in the retail sector.

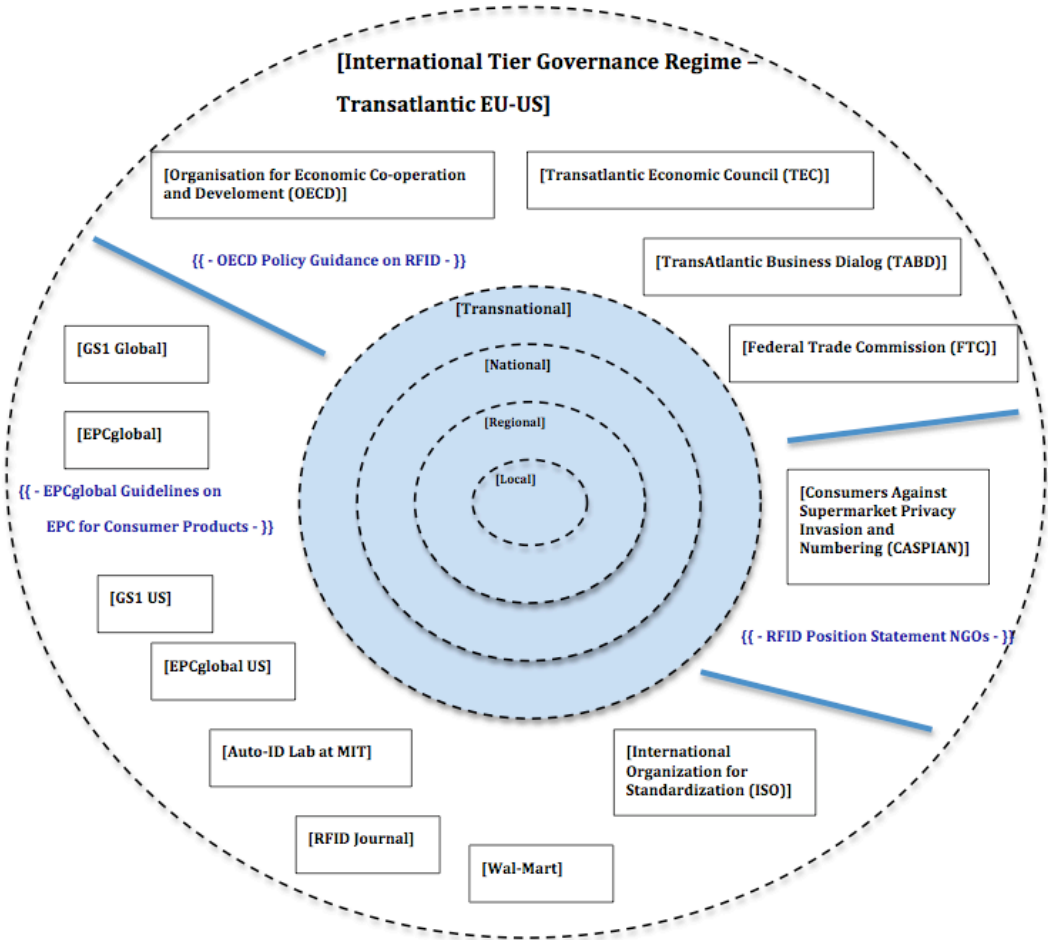


Figure 22 - International tier arena of the emerging governance regime for consumer privacy in retail

5.5.1 Transatlantic dialogs

5.5.1.1 EU-US Summit Declaration¹¹¹

On 30 April 2007 the EU-US Summit Declaration was signed in Washington DC.¹¹² The leaders of the EU and US stated that better transatlantic economic integration between the EU-US would be beneficial to citizens and competitiveness of both economies (Summit, 2007). The Summit Declaration identifies several ‘Lighthouse Priority Projects’ that aim at stimulating this transatlantic economic integration for boosting economic growth on both sides. One of them is the Innovation and Technology ‘Lighthouse Priority Project’ in which RFID is singled out as a key area for joint action. The Summit Declaration states the following regarding joint RFID action between the EU and the US: ‘Develop a joint framework for cooperation on identification and development of best practices for Radio Frequency Identification (RFID) technologies’ (Summit, 2007: 11) and ‘Exchange best practices on all dimension related to RFID’ (Summit, 2007: 17). The Transatlantic Economic Council (TEC)¹¹³ being instituted simultaneously has the task to supervise and coordinate the identified Lighthouse Priority Projects.

Within the context of the ‘TEC Lighthouse Priority Project on RFID’, the first EU-US symposium on RFID entitled: ‘Transatlantic Symposium on the Societal Benefits of RFID’ took place in Washington D.C on 22 September 2008 (TABD, 2008). This symposium was co-hosted by the TransAtlantic Business Dialogue (TABD)¹¹⁴, European-American Business Council (EABC)¹¹⁵, and EPCglobal¹¹⁶, with the support of the US Department of Commerce¹¹⁷ and the Information Society and Media Directorate-General of the European Commission (DG INFSO).¹¹⁸ The main objective of this symposium was to encourage a dialog between transatlantic stakeholders from business, consumer, and governmental organizations on the development of RFID. The symposium made clear that the EU and the US strive for harmonizing consumer privacy and data protection regulation with regard to RFID. In addition, the ‘OECD Policy Guidance on RFID’ was adopted as a best practice recommendation for RFID-specific regulation. During this symposium, the METRO Group as the only pioneer of RFID on item-level tagging presented a case study of their RFID pilot projects within their Future Store Initiative. A second follow-up Transatlantic EU-US Symposium on the Societal Benefits of RFID was scheduled for Brussels on the 5th and the 6th of May 2009.¹¹⁹

In conclusion, the transatlantic dialog between the EU and the US concerning RFID-specific regulation has been institutionalized within the ‘TEC Lighthouse Priority Project on RFID’.

¹¹¹ This section is a synthesis based upon: Summit, 2007; EC-Sym, 2008; TABD, 2008, and my attendance to the ‘Transatlantic Symposium on the Societal Benefits of RFID’ on 22 September 2008.

¹¹² The EU-US Summit declaration of 30 April 2007 was signed by Mr. George W. Bush, president of the U.S., Mss Angela Merkel Chancellor of Germany and Mr. José Manuel Barroso, president of the European Commission.

¹¹³ For more information about the Transatlantic Economic Council (TEC) consult: <http://www.eurunion.org/partner/euusrelations/TEC.htm> and http://ec.europa.eu/enterprise/international_relations/cooperating_governments/usa/usa_tec_en.htm.

¹¹⁴ For more information about the TransAtlantic Business Dialogue (TABD) consult: <http://www.tabd.com/>.

¹¹⁵ For more information about the European-American Business Council (EABC) consult: <http://www.eabc.org/>.

¹¹⁶ For more information about EPCglobal consult: <http://www.epcglobalinc.org/>.

¹¹⁷ For more information about the U.S. Department of Commerce consult: <http://www.commerce.gov/>.

¹¹⁸ For more information about the Information Society and Media Directorate-General of the European Commission (DG INFSO) consult: http://ec.europa.eu/dgs/information_society/.

¹¹⁹ For more information about the second transatlantic lighthouse symposium on RFID consult: http://ec.europa.eu/information_society/policy/rfid/events/index_en.htm.

5.5.1.2 The Federal Trade Commission¹²⁰

On 23 September 2008, coupled with the first Transatlantic symposium as explained in the previous section, the first ‘Transatlantic RFID Workshop on Consumer Privacy and Data Security’ was organized by the Federal Trade Commission (FTC)¹²¹ and the DG INFSO in Washington D.C (FTC, 2008c). In the US, the FTC is the organization that concerns itself with consumer privacy protection. In the US, most of the RFID-specific regulation is established on the State level and usually only covers certain RFID-specific applications or sectors (NCSL, 2008). The FTC as the consumer interest authority in the US therefore has the task to investigate whether RFID-specific regulation on the Federal level is required to warrant consumer privacy.

In order to investigate the need for RFID-specific regulation on the Federal level in the US, the FTC already organized a workshop on RFID entitled: ‘RFID – Radio Frequency Identification: Applications and implications for Consumers’ on 21 June 2004 (FTC, 2004). This workshop included panel discussions amongst stakeholders from business, consumer, and governmental organizations in the US. The FTC concluded that the need for RFID-specific privacy legislation on the Federal level was not required. However, to alleviate RFID-specific privacy and security concerns among consumers, the FTC, based upon the workshop, made the following recommendations: transparency of RFID applications, sound database security measures, increasing consumer education of RFID, and industry self-regulation supplemented with accountability provision to ensure compliance (FTC, 2005).

The FTC also contributed to the EC Public Online Consultation on the draft text of the EC ‘RFID Privacy, Data Protection and Security Recommendation’ (FTC, 2008a). The essence of the FTC comments is that they support the risk-based approach the EC is taking towards potential consumer privacy and data security issues of RFID. In particular, the FTC supports consumer awareness raising activities for RFID. Nevertheless, as the FTC adopts a more flexible, risk-based approach to privacy and data security, the FTC encourages effective industry self-regulation coupled with the enforcement of existing legislation. Because the RFID technology is still an emerging technology, especially in the retail sector on consumer products, the FTC conceives the RFID-specific regulation as proposed in the EC ‘RFID Privacy, Data Protection and Security Recommendation’ to be premature. The FTC conceives the existing consumer privacy and security legislation and their consumer protection statute, Section 5 of the FTC Act¹²², to cover all the potential risks of RFID for consumer privacy in the US (FTC, 2008a).

In conclusion, the FTC thinks that RFID-specific regulation for is not necessary at the moment and therefore they disagree with the position the EC takes on this point.

¹²⁰ This section is a synthesis based upon: FTC, 2004; FTC, 2005; FTC, 2008a; FTC, 2008c; NCSL, 2008, and my attendance to the ‘Transatlantic RFID Workshop on Consumer Privacy and Data Security’ on 23 September 2008 and email correspondence with Kathryn Ratté (FTC).

¹²¹ For more information about the Federal Trade Commission (FTC) consult: <http://www.ftc.gov/>.

¹²² For more information about the FTC Act and the consumer protection statute (15 U.S.C. §§ 41-57) consult: <http://www.ftc.gov/ogc/ftcact.shtml>.

5.5.2 The OECD as a high-level policy guide¹²³

Additional to the transatlantic dialogs between the EU and the US, the Organization for Economic Co-operation and Development (OECD)¹²⁴ plays an important role in stimulating the harmonization of consumer privacy legislation and the emerging RFID-specific regulation between the EU and the US. In fact the ‘RFID Privacy, Data Protection and Security Recommendation’ adopts and therefore harmonizes with the ‘OECD Policy Guidance on RFID’ adopted on 18 June 2008 (OECD, 2008). The ‘OECD Policy Guidance on RFID’ is based upon the technology-neutral OECD Privacy Guidelines of 23 September 1980 and OECD Security Guidelines of 25 July 2002. Table 11 below provides a comprehensive overview of these key policy outcomes and events in the policy-making processes of the OECD that resulted in the adoption of the ‘OECD Policy Guidance on RFID’ on 18 June 2008.

In the period between 2005 and 2008 (see table 11 below), the Committee for Information, Computer and Communications Policy (ICCP)¹²⁵ of the Directorate for Science, Technology and Industry (DSTI)¹²⁶ of the OECD has been conducting the work on RFID-specific regulation. The aim of the ICCP is to devise policies that maximize the benefits as offered by the Information Society. The work of the ICCP on RFID originated in 2005 at the ICCP Foresight Forum on RFID that included stakeholders from government, academia, private sector, and civil society (NGOs). The ICCP concluded that in order the economical potential for businesses and consumers (benefits) of RFID to be realized in the future, information security and privacy concerns (challenges) of RFID need to be addressed. Consequently, the Working Party on Information Security and Privacy (WPISP) and the Working Party Information Economy (WPIE) of the ICCP started working on both the economical aspects and the privacy and security aspects of RFID. The ICCP committee and its working parties involved OECD member countries, observers, and representatives from the business community and civil society to devise analytical studies on RFID. The formulation of the ‘OECD Policy Guidance on RFID’ is based upon these analytical studies. The analytical studies of the ICCP are declassified which indicates a consensus at the level of the committee. Consequently, the work of the ICCP on the ‘OECD Policy Guidance on RFID’ was taken upon in the policy framework adopted at the ‘OECD Ministerial Meeting on the Future of the Internet Economy’ in Seoul Korea on 17-18 June 2008.¹²⁷ The ‘OECD Policy Guidance on RFID’ therefore is a balanced document as it is based upon the analytical reports and reflects a consensus shared by the OECD member countries, businesses, and civil society.

The ‘OECD Policy Guidance on RFID’ is considered final, although its last principle indicates to monitor its evolution (principle 14). Nevertheless, the work on the Guidance is not going to be re-opened, as the ICCP is currently continuing its work on RFID within a broader topic called ‘sensor-based environments and ubiquitous networks’, equivalent with the ‘Internet of Things’ (IoT). Overall, the OECD has a high-level policy approach towards RFID issues and employs its own instruments in devising RFID-specific policies. As a result, the Guidance provides high-level policy guidance. It sets 14 high-level policy principles that

¹²³ This section is a synthesis based upon: OECD, 2008 and email correspondence with Laurent Bernat and Karine Perset (OECD).

¹²⁴ For more information about the Organization for Economic Co-operation and Development (OECD) consult: http://www.oecd.org/home/0,3305,en_2649_201185_1_1_1_1_00.html.

¹²⁵ For more information about the Committee for Information, Computer and Communications Policy (ICCP) of the DSTI of the OECD consult: http://www.oecd.org/department/0,3355,en_2649_34223_1_1_1_1_00.html.

¹²⁶ For more information about the Directorate for Science, Technology and Industry (DSTI) of the OECD consult: http://www.oecd.org/department/0,3355,en_2649_33703_1_1_1_1_00.html.

¹²⁷ For more information about the ‘OECD Ministerial Meeting on the Future of the Internet Economy’ including analytical studies, policy recommendations and guidances and speakers from the 30 OECD Member States and the EC consult: www.oecd.org/FutureInternet.

can be employed by policy makers in their own policy-making process that often takes place at a more detailed level, i.e. on more specific matters of concern. Hence, as the scope of the Guidance is broad, it does not provide any solutions to the ‘opt-in vs. opt-out’ issue in the European retail sector. Nevertheless, the awareness and information (principle 4), standards (principle 5), Privacy Impact Assessment (PIA) (principle 8) and the Privacy-Enhancing-Technologies (PET) privacy-by-design (principle 9) are clearly incorporated in the EC ‘RFID Privacy, Data Protection and Security Recommendation’. The EC Recommendation is more concrete on the RFID applications in the retail sector. Finally, the Guidance encourages a continued dialog between all stakeholders (principle 13), something that is fully engrained in the practices of the EC in finalizing their ‘RFID Privacy, Data Protection and Security Recommendation’.

Year	Date	Outcome or Event	Description
1980	- 23 September 1980	- Technology-neutral policy recommendation	- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ¹²⁸
2002	- 25 July 2002	- Technology-neutral policy recommendation	- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security ¹²⁹
2005	- 05 October 2005	- OECD Foresight Forum (conference)	- OECD Foresight Forum entitled: 'Radio Frequency Identification (RFID) Applications and Public Policy Considerations' organized in Paris. ¹³⁰ The conference involved stakeholders from government, academia, private sector and NGOs.
2006	- 07 February 2006	- OECD Foresight Forum Proceedings	- Proceedings of the OECD Foresight Forum on Radio Frequency Identification Applications and Public Policy Considerations. This study contains the proceedings of the OECD Foresight Forum on Radio-Frequency Identification (RFID) that was held in Paris on October 2005 (DSTI/ICCP(2006)7) ¹³¹
	- 27 February 2006	- Analytical study regarding RFID	- Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations (DSTI/ICCP(2005)19/FINAL) ¹³²
2007	- 27 November 2007	- Analytical study regarding RFID	- Radio Frequency Identification Implementation in Germany: Challenges and Benefits (DSTI/ICCP/IE(2007)6/FINAL) ¹³³
2008	- 14 January 2008	- Analytical study regarding RFID	- Radio-Frequency Identification: a Focus on Security and Privacy (DSTI/ICCP/REG(2007)9/FINAL) ¹³⁴
	- 18 April 2008	- Analytical study regarding RFID	- RFID Applications, Impacts and Country Initiatives (DSTI/ICCP/IE(2007)13/FINAL) ¹³⁵
	- 17-18 June 2008	- RFID-specific policy recommendation	- OECD Policy Guidance on Radio Frequency Identification (RFID) ¹³⁶ adopted on the OECD Ministerial Meeting on the Future of the Internet Economy ¹³⁷

Table 11 – RFID-specific policy outcomes/events in the policy-making process orchestrated by the OECD using their policy-making instruments between 2005-2008

¹²⁸ This document is available at: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

¹²⁹ This document is available at: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

¹³⁰ More information about the OECD Foresight Forum entitled: Radio Frequency Identification (RFID) Applications and Public Policy Considerations' consult: http://www.oecd.org/document/58/0,3343,en_2649_34223_35186234_1_1_1_1,00.html.

¹³¹ This document is available at: <http://www.oecd.org/dataoecd/59/12/36069207.pdf>.

¹³² This document is available at: <http://www.oecd.org/dataoecd/57/43/36323191.pdf>.

¹³³ This document is available at: [http://www.olis.oecd.org/olis/2007doc.nsf/ENGDATCORPLOOK/NT0000481A/\\$FILE/JT03237310.PDF](http://www.olis.oecd.org/olis/2007doc.nsf/ENGDATCORPLOOK/NT0000481A/$FILE/JT03237310.PDF).

¹³⁴ This documents is available at: [http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/\\$FILE/JT03238682.PDF](http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/$FILE/JT03238682.PDF).

¹³⁵ This document is available at: <http://www.oecd.org/dataoecd/6/12/40536990.pdf>.

¹³⁶ This document is available at: <http://www.oecd.org/dataoecd/19/42/40892347.pdf>.

¹³⁷ For more information about the 'OECD Ministerial Meeting on the Future of the Internet Economy' including the 'The Seoul Declaration for the Future of the Internet Economy' and the 'Shaping policies for the future of the Internet Economy' consult: www.oecd.org/FutureInternet.

5.5.3 Conclusion

In this section, we saw that the EU and the US within a transatlantic dialog and on their own have a deliberative approach. They pursue to involve all the relevant stakeholders from business, consumer, and government organizations in the public debate about RFID and the development of RFID-specific regulations. Nevertheless, there are several differences in the regulatory processes between the EU and the US. The EC clearly takes a proactive approach in the development of RFID-specific regulation to address consumer privacy concerns. The US on the other hand takes a more reactive approach, as the US encourages industry self-regulation instead of the development of Federal RFID-specific regulation. In addition, the EC with their 'RFID Privacy, Data Protection and Security Recommendation' pursues to harmonize the regulatory frameworks of the EU Member States. The US on the other hand has no Federal RFID-specific regulation as RFID-specific regulation is codified at the State level that differs greatly. In other words, the US approach towards RFID-specific regulation is more scattered and bottom-up whereas the EU approach is more harmonizing and top-down.

The differences between the EU and the US are also reflected in the research projects towards RFID, which is government-driven in the EU and market-driven in the US. The EU has sound RFID research projects between governmental agencies and industry in the Cluster European RFID Projects (CERP). The US on the other hand does not have Federal sponsored RFID research projects in cooperation with industry. In the US, research towards RFID is more market-driven and is carried out by individual research institutes and private companies (Roberti, 2008).

Within the context of the 'TEC Lighthouse Priority Project on RFID', initiated by the EU-US Summit Declaration of 2007, transatlantic dialogs between the EU and US take place. These dialogs allow for the constant re-evaluation and adjustments to make the regulatory frameworks concerning RFID of the EU and US compatible for trade and economic growth. The OECD plays an important role in these transatlantic dialogs too. The ICCP committee of the OECD used its own policy-making instruments for developing the 'OECD Policy Guidance on RFID'. The Guidance provides a set of high-level policy principles that policy-makers can draw upon. Consequently, the draft version of the EC 'RFID Privacy, Data Protection and Security Recommendation' has adopted and integrated several of its principles. Nevertheless, in the transatlantic context the 'opt-in vs. opt-out' issue remains unresolved.

5.6 Local tier of the governance regime revisited – The METRO Group Future Store Initiative phase two (METRO 2) (Q1-Q4)

5.6.1 The METRO Group and their partners in the Future Store Initiative

Since 2003, the METRO Group Future Store Initiative (MGFSI) as a joint RFID-driven R&D platform coordinated by the METRO Group expanded its partner organizations and its activities. Currently, the MGFSI includes more than 90 partners from the Information Technology (IT) sector, retail sector, and academia (MGFSI, 2009). Figure 23 below shows that the MGFSI has divided their current partners companies in a hierarchical manner.

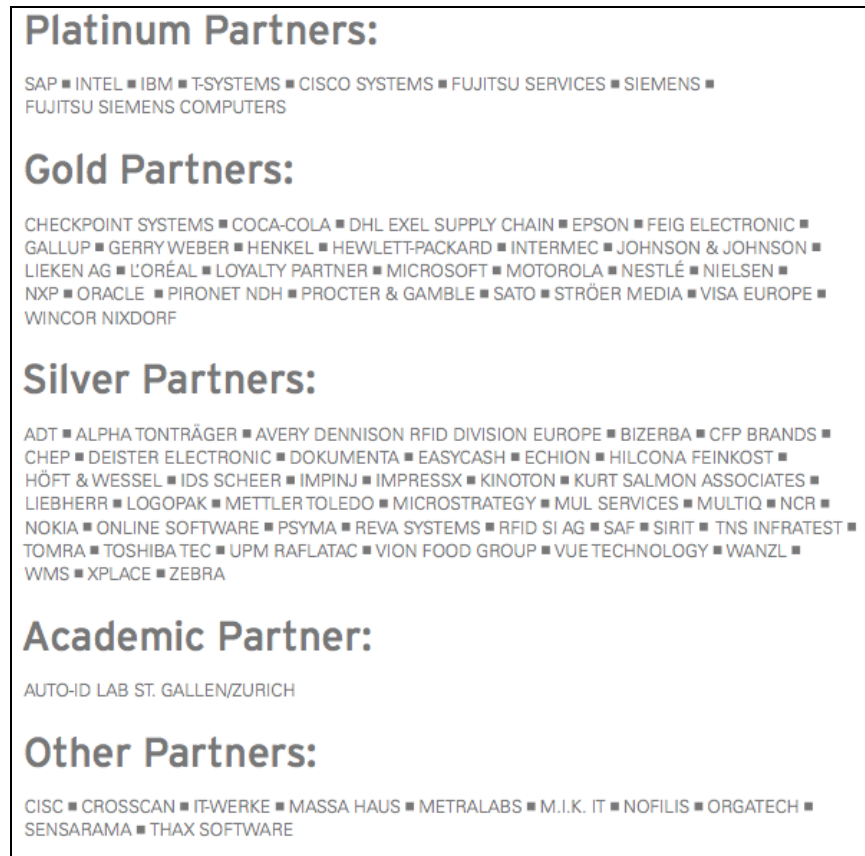


Figure 23 - Partner organizations of the MGFSI (MGFSI, 2008: 36)

5.6.2 Current RFID pilot projects of the METRO Group Future Store Initiative

Three years after the consumer privacy controversy of their first RFID pilot project in the Future Store in Rheinberg, i.e. ‘METRO 1’, the MGFSI launched two new RFID pilot projects on the local tier in Nordrhein-Westfalen (NRW), i.e. ‘METRO 2’. The METRO Group RFID Innovation Center in Neuss, the real-life exhibition and test lab for the MGFSI, has been continuing its operations since its inception in 2004.

5.6.2.1 The Gardeur-Galeria Kaufhof in Essen¹³⁸

On 20 September 2007, the MGFSI started their RFID pilot project in the men’s fashion department of the Galeria Kaufhof department store in Essen.¹³⁹ Their aim was to improve the efficiency of the supply chain and to enhance customer service and shopping experience. RFID was rolled out on all the clothing items on the men’s department floor and in particular the Gardeur-brand-shop. The RFID pilot project is sponsored by the Building Radio frequency IDentification solutions for the Global Environment (BRIDGE) project within the Cluster of European RFID Projects (CERP) of the EC.¹⁴⁰

The RFID pilot project consists of four RFID-enabled smart dressing rooms, three smart display tables, one smart mirror, smart clothing racks, and two smart shelves. In addition, it is the first end-to-end EPC Gen. 2 class 1 UHF item-level application. RFID readers are installed on the transshipment points that enable the seamless integration of the back-end and front-end of the department store. Inside the department store, there are about 100 antennas and about 60 RFID near-field UHF readers/interrogators that are suitable for a dense RFID environment to prevent cross reading. This is needed because on an area of about 2000 square meter about 30.000 clothing items are provided with the EPC Gen. 2 class 1 RFID labels. These are attached to the clothing in the Distribution Center (DC) of Galeria Kaufhof in Neuss. This is the same building that hosts the METRO Group RFID Innovation Center and the European EPC Competence Center (EECC).

Inside the department store, the smart clothing racks contain a RFID tag as well. These are linked with the ID of the apparel they store. In this way, it is possible to analyze which racks sell well and which do not, i.e. analyzing the performance of the merchandise presentation to the customers. Furthermore, inventory management is easy, convenient, and fast with the handheld RFID reader that is connected to the back-end IT infrastructure. The IT system knows exactly what is coming in from the DC and what is coming through from the back room to the sales floor. In this way, the RFID pilot project gains unprecedented efficiency and transparency of the goods travelling through the supply chain from the DC to the sales floor. Out-of-stocks therefore is a thing of the past, as they are able to carefully tailor supply and demand. Customers benefit from RFID by means of the RFID-enabled smart display tables and the smart shelves that allow instant information about the availability and location of their desired clothing items. In addition, the smart dressing rooms, which are provided with an interactive RFID-enabled flat screen, and the smart mirror, provide information about the clothing items, such as the item’s picture, size, color, price, material, care instructions, and suggestions for matching clothing items.

At the checkout, the pilot project is running the barcode system with barcode scanners and labels attached to consumer products together with the EPC/RFID system to compare performance. The EPC/RFID tags on the consumer products can be easily removed at the checkout when customers ask for it, i.e. conform the ‘opt-out principle’. If customers do not

¹³⁸ This section is a synthesis based upon: MGFSI, 2009; METRO Group 2007; Wessel, 2007; and the guided tour I took at the Galeria Kaufhof in Essen on 04 July 2008.

¹³⁹ For more information about the RFID pilot projects of the MGFSI in the Galeria Kaufhof consult: <http://www.future-store.org/fsi-internet/html/en/1613/index.html>.

¹⁴⁰ For more information about the BRIDGE Project consult: <http://www.bridge-project.eu/>.

'opt-out' the RFID tags can function as digital receipts for easy product recall. Customers are fully informed about the RFID pilot project, as there are information boards and brochures available. Besides customers, the employees also need to be educated about the EPC infrastructure. The pilot project pursues to incorporate the customer and the employee in the development of the RFID infrastructure. In December 2008, the pilot ended and the data is currently being analyzed by the MGFSI.

5.6.2.2 The REAL Future Store in Toenisvorst¹⁴¹

On 28 May 2008, the MGFSI started their second RFID pilot project in Toenisvorst. Here they opened the REAL Future Store, a supermarket and successor of the first Future Store in Rheinberg (METRO 1). The REAL Future Store in Toenisvorst is meant for an enhanced convenient, self-service, and one-stop-shopping-experience. Customers are exposed to cutting-edge technologies and novel retail concepts. These include interactive terminals and tasting stations, such as the interactive skincare information terminal and the wine tasting station. Furthermore, the mobile shopping assistant, self-checkouts, smart scales, multi-media terminals, ambient sound, ambient scent, and a pay by fingerprint system are part of the package.¹⁴²

As the METRO Group is leading with the RFID technology, the REAL Future Store contains a RFID pilot project as well. In the REAL Future Store RFID is rolled out in the 'The Master Butcher Shop¹⁴³', for the demand-driven production of meat products. After production, the meat products are packaged in RFID-tagged foam trays and are transported to a smart freezer (RFID-enabled refrigerator). The RFID tags are passive EPC Gen. 2 class 1 UHF transponders. The smart freezer consists of 50 compartments and is about 30 to 40 meters in length, 1.5 meter in depth, and 1.5 meters in width. The smart freezer contains 50 RFID readers and about 200 antennas. This RFID-enabled system facilitates the inventory control and quality assurance of the self-service smart freezer. It enables the tracking of individual meat packages and the monitoring of the stock levels and best before dates of products in the smart freezer. In this way the production and the demand of customers for meat products is balanced, without the need for manual check-ups. Consequently, product availability (no out-of-stocks), no waste (no over production), and product quality/safety for consumers (no expired meat products sold) is assured. Therefore, this RFID application is a clear example of a win/win situation in which customers as well as the retailer benefit.

The checkout of the REAL Future Store is running on the barcode system. Neither personal data is stored on the RFID tags (only the EPC number), nor RFID tags are linked with personal data at the checkout. In addition, customers are able to permanently deactivate the tags beyond the point of sale by using the two RFID-deactivators stations that are installed at the exit of the in Future Store. Furthermore, the REAL Future Store provides clear consumer notice by EPC/RFID logos on products and readers, and they provide information brochures. Over the last 5 years on average one customer per week decided to deactivate the RFID tag on the products. The METRO Group has received no formal complains and only a couple of customers have voiced their concern (EC-Sym, 2008).

¹⁴¹ This section is a synthesis based upon: MGFSI, 2009; METRO Group, 2008; Swedberg, 2008, and the guided tour I took at the REAL Future Store in Toenisvorst on 02 July 2008.

¹⁴² For more information including a comprehensive and detailed overview of all the different innovative retail technologies that are operation in the REAL Future Store in Toenisvorst consult: <http://www.future-store.org/fsi-internet/html/en/375/index.html>.

¹⁴³ For more information about the RFID application in the 'The Master Butcher shop' in the REAL Future Store in Toenisvorst consult: <http://www.future-store.org/fsi-internet/html/en/7626/index.html>.

5.6.3 The visible implementation of RFID-specific regulation¹⁴⁴


According to Thiesse, in respect to ‘METRO 1’ the MGFSI in ‘METRO 2’ is communicating more proactively to their customers and to the public at large about their RFID activities and their privacy policy. In addition, the Public Relations (PR) of the MGFSI has become far more professional than it was at the time of ‘METRO 1’.

Indeed, ‘METRO 2’ visibly implements the emerged multi-tier and multi-actor RFID-specific regulations for consumer privacy protection to show that they warrant consumer privacy. Firstly, the pilot projects implement the ‘EPCglobal Guidelines for EPC on Consumer Products’. The MGFSI, operationalized the EPC Guidelines within the context of their RFID pilot projects, i.e. they created their own privacy policy in line with the EPCglobal Guidelines, see figure 24 below. Secondly, the RFID pilot projects fully comply with the German and European data protection legislation, respectively the German ‘Data Protection Act’ (BDSG) and the ‘Data Protection Directive (95/46/EC)’. Thirdly, the MGFSI implements the draft version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’. As described in the section about Nordrhein-Westfalen (NRW), the MGFSI followed the draft EC Recommendation and voluntarily executed a Privacy Impact Assessment (PIA) that was approved upon by the Data Protection Supervisory Authority in Nordrhein-Westfalen (NRW). Finally, the MGFSI transparently and comprehensively provides information about their RFID activities by means of RFID newsletters, brochures, an Internet site, and even a RFID hotline. Figure 24 below summarizes the consumer privacy policy and information provisions of the METRO Group concerning their RFID activities that they communicate to their customers.

EPC global guidelines at the METRO Group


The METRO Group utilises RFID on the basis of the Electronic Product Code (EPC). Standards of other providers are not recorded. If a supplier decides to deploy RFID (wether using EPC or not) he is requested to inform the METRO Group. A number code (EPC) os stored on the RFID transponders (Smart Chips), as used by the METRO Group. This encrypts information on logistic units, products or processes. This data can be recorded without contact using an RFID reading device. Authorized users can then access product and process-relevant data (e.g. product name, manufacturer, country of origin) via a database.

1 NOTIFICATION




- Comprehensive information on the deployment of RFID technology within METRO Group:
- On the Internet at www.metrogroup.de, www.future-store.org
- Direct queries by e-mail to rfid@metro.de or via the hotline: +49 (0)211.68 86-20 04
- In the METRO Group RFID Newsletter
- In brochures, e.g. "The METRO Group and RFID," "METRO Group RFID Innovation Center" and "METRO Group Starter Kits"
- Open dialog with special interest groups and experts, e.g. membership of the Informationsforum RFID e.V.

2 INFORMATION




- Customer information as to where RFID is deployed, for example, on written notices on the sales floor
- Marking of all logistic units, cartons and products equipped with Smart Chips with the EPC logo as well as extra written information
- Marking of all RFID readers

3 FREEDOM OF CHOICE



- Customers can permanently disable and remove Smart Chips on products after payment.
- The METRO Group is involved in the development of new deactivation technologies, e.g. the De-Activator.

4 DATA PROTECTION



- The German Data Protection Act (BDSG) will be upheld at all times in the implementation of EPC within METRO Group.
- EPC refers to product and process-related information only. No personal data is saved.
- METRO Group only uses RFID transponders that comply with EPC standards.
- There is no relationship between EPC and personal data. As a rule this can only take place with the customer's permission. However, anonymity is always guaranteed when paying by cash.

Figure 24 - EPCglobal Guidelines implement at the MGFSI (MGFSI, 2009b)

¹⁴⁴ This section is a synthesis based upon: MGFSI, 2009a; MGFSI, 2009b, the guided tours I took at the REAL Future Store in Toenisvorst (02 July 2008) and the Galeria Kaufhof in Essen (04 July 2008), and email correspondence with Frederic Thiesse (Auto-ID labs University of St. Galen).

5.6.4 Conclusion

The METRO Group (EPC technology user) together with their IT partners (EPC technology producers) and retail partners (consumer products suppliers) in the MGFSI are the prominent host of RFID pilot projects on consumer products (CPILT) in the EU. In ‘METRO 1’, no RFID-specific regulation for consumer protection was implemented. In contrast, in ‘METRO 2’ it is clear that RFID-specific regulation is implemented. ‘METRO 2’ fully complies with the ‘EPCglobal Guidelines for EPC on Consumer Products’, the German ‘Data Protection Act’ (BDSG), the ‘Data Protection Directive (95/46/EC)’, and the *draft* version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’. Hence, the RFID pilot projects of the MGFSI on the local tier in Nordrhein-Westfalen (NRW) are the *loci* of the visual and tacit manifestation of the implementation and evaluation of the emerged multi-actor and multi-tier RFID-specific regulation for consumer privacy protection.

The MGFSI therefore plays a pivotal role in stimulating the public debate and the learning that takes place regarding the functioning of the newly developed RFID-specific regulation for consumer privacy protection. This as the RFID pilot projects of the MGFSI take place under real-life conditions and hence are open to the public, including consumers and consumer interest NGOs. The consumer interest groups in Germany closely watch the current RFID pilot projects of the MGFSI. However, no issues with consumer privacy have been reported. The MGFSI therefore shows that sound RFID-specific regulation can make or break RFID for the application on consumer products. Nevertheless, the ‘opt-in vs. opt-out’ issue still needs to be resolved by the *final* version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’. For now the RFID pilot projects of the MGFSI implement the ‘opt-out principle’. Eventually, the MGFSI needs to implement the final EC ‘RFID Privacy, Data Protection and Security Recommendation’. It therefore needs to be seen whether the application of RFID on consumer products will be continued in the future, as the ‘opt-in’ requirement is a no-go area for the retail sector.

In conclusion, between 2003 and 2007 in the *RFID technological niche (GSI-EPCglobal-EPC)*, the MGFSI learned how to *use* and *produce* the RFID technology on consumer products. Between 2005 and 2009, the MGFSI being part of the multi-tier and multi-actor emerging governance regime for consumer privacy protection, also learned how to *regulate* the application of RFID on consumer products. In figure 25 below the current local tier arena of the emerging governance regime for consumer protection is depicted.

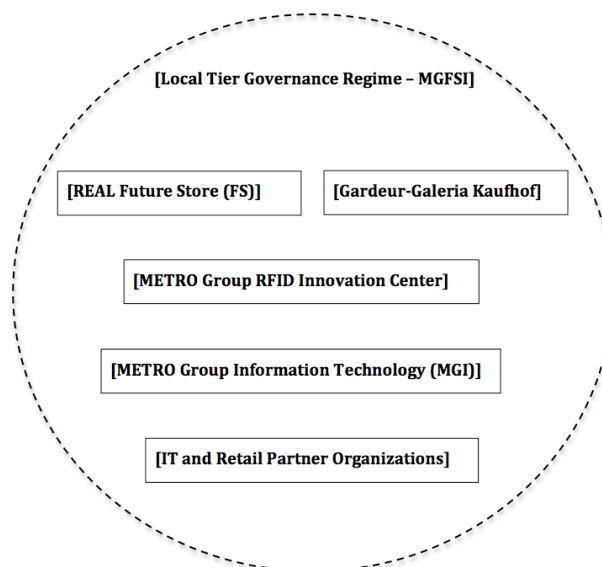


Figure 25 - Local tier arena of the emerging governance regime for consumer privacy protection in retail

5.7 Conclusion

This chapter showed that in tandem with the emerging application of RFID on consumer products, an emerging governance regime for consumer privacy protection for RFID in retail emerged, i.e. an emerging regulatory capability for the application of RFID on consumer products in the retail sector. The emerging governance regime consists of multi-tier and multi-actor interconnected though parallel operating policy arenas. The RFID-specific regulatory outcomes build upon the EPCglobal industry voluntary self-regulation initiative that resulted in a code of conduct for the global EPC industry in the embodiment of the 'EPCglobal Guidelines for EPC on Consumer Products' of 1 January 2005. These EPC Guidelines were a reaction of the global EPC industry (EPC technology users and producers) to the consumer privacy controversies of RFID applied on consumer products in the retail sector. In addition, they were a reaction to the shared RFID Position Statement as published by EU and US consumer privacy and liberty NGOs on 20 November 2003.

Germany as a forerunner in the development and application of RFID in the EU plays an important role in the development of RFID-specific regulation. Between 2005 and 2009, after the consumer privacy controversy of 'METRO 1', we saw different RFID-specific regulatory processes and outcomes on different tiers in the EU and in particular in Germany. The RFID-specific regulatory processes took place against the backdrop of the technology-neutral data protection legislation that is intertwined on the regional, national, and transnational tier. Similarly, the development of RFID-specific regulation also takes place in an intertwined and multi-tier fashion. In Germany, the role of institutions on the regional tier of Nordrhein-Westfalen (NRW) is primarily, supervising, monitoring, and gathering information of the RFID pilot projects of the MGFSI, to be passed on to the relevant organizations on the national and transnational tier. On the national tier of the Federal Republic of Germany, the 'Düsseldorfer Kreis' published the first RFID-specific regulatory 'Recommendation on RFID' on 8/9 November 2006. In addition, between 2005 and February 2008, there was the 'three staged self-regulation initiative' between private and public stakeholders for a code of conduct for the EPC industry. The negotiations deadlocked on the 'opt-in vs. opt-out' issue and this core issues was passed on to the German Government and the EC. On 23 January 2008, the German Government published the 'Report German Government on RFID regulation' that encouraged industry-self regulation and to wait for the EC to publish their final 'RFID Privacy, Data Protection and Security Recommendation'. In other words, the German Government decided not to resolve the 'hot potato' of 'opt-in vs. opt-out', but recommended to wait for the EC. Consequently, the German Government and stakeholders in the industry self-regulation initiative are waiting for the EC.

Since 2005, the EC as the top-moderator in the EU has been working on the development of RFID-specific regulation within the i2010 ICT policy framework. The activities of the EC culminated in the publication of the draft version of 'RFID Privacy, Data Protection and Security Recommendation' on 21 February 2008. On the international tier, there are regulatory processes as well. After the EU-US Summit Declaration of 30 April 2007, RFID as a 'TEC RFID Lighthouse Priority Project' has been identified as a key area of joint action for stimulating economic integration between the EU and the US. Consequently, a constant dialog between the EU and US followed on RFID in conferences and workshops to harmonize the RFID-specific regulatory frameworks. Furthermore, on 17 June 2008 the OECD adopted the 'OECD Policy Guidance on RFID', following their initial work on RFID dating back to 2005. Besides the transatlantic dialog between the EU and US, the OECD plays a key role in harmonizing international RFID-specific regulation. The policy harmonization initiatives serve the purpose of smoothing possible trade barriers and stimulating the development of both economies. All these multi-tier and multi-actor RFID-

specific regulatory processes and outcomes converge to the final EC 'RFID Privacy, Data Protection and Security Recommendation'. This will be an official RFID-specific legal instrument to be transposed in the legislation of the EU Member States.

The RFID-specific regulation is imposed upon and implemented in 'METRO 2', the recently launched RFID pilot projects of the METRO Group in their Future Store Initiative. So far, no consumer privacy issues with RFID on consumer products have been reported. Nevertheless, the core issue of 'opt-in vs. opt-out' is still open. The EC expects to publish the final EC 'RFID Privacy, Data Protection and Security Recommendation' in Spring 2009. The Recommendation will disclose whether 'opt-in' or 'opt-out' is going to be required as the standard in retail. The result could mean the end of RFID on item-level tagging in the European retail sector, as 'opt-in' is a definite no-go area for the EPC industry.

Next chapter will reflect upon these empirical findings of the RFID governance case study in the light of the hybrid MLP-GP conceptual framework to answer conceptual-laden research questions Q4-Q7.

6. Discussion – Understanding the emerging RFID-specific regulatory capability in socio-technical transition

This chapter presents the discussion that interprets the empirical findings, as presented in RFID governance case study in the previous two chapters, in the light of the hybrid MLP-GP analytical framework as presented in chapter two. In doing so, this chapter answers the conceptual-laden research questions Q4-Q7. Section 6.1 interprets the empirical findings of the emerging governance regime for consumer privacy protection of RFID in terms of different modes of governance. Then section 6.2 interprets the empirical patterns in terms of the socio-technical transition pathways of the MLP. Section 6.3 then presents the policy recommendation for the empirical field. Finally, section 6.4 puts forward and discusses the conceptual contributions and refinements of this study.

6.1 Different modes of governance (Q4)

The RFID governance case study presented as well *the need for*, and *the actual* emerging regulatory capability for consumer privacy protection of RFID in the European retail sector. The emerging regulatory capability was conceptualized in terms of the governance dynamics in an emerging multi-tier and multi-actor governance regime. This section will characterize the policy outcomes for collective action concerning consumer privacy protection that are the resultants of the policy processes of collective decision-making of this complex emerging governance regime. In doing so, this section will draw upon the defined modes of governance that describe the structures and interactions of the organized actors in an arena as provided by Benz (2006) and summarized in chapter two.

The first RFID-specific consumer privacy regulatory outcome emerged in the form of the EPCglobal voluntary industry self-regulation initiative for a code of conduct for the EPC industry entitled: ‘EPCglobal Guidelines for EPC on Consumer Products’ of 1 January 2005. The EPCglobal Guidelines were a reaction to the consumer privacy controversies with EPC applied on consumer products in the retail sector and the shared RFID Position Statement of EU and US consumer privacy NGOs published on 20 November 2003. The mode of governance that best describes the structure and interactions of the involved actors in the EPCglobal arena is the ‘network’ structure. The network structure is characterized by the more or less symmetrical relationships amongst the actors, in this case the business partners in the EPCglobal network. The business partners of the EPCglobal mutually adjust towards each other for the coordination of actions within their collective cooperative orientation that is based upon trust to make the EPC standards suite succeed. The outcome of the policy-making process maintained by the Public Policy Steering Committee (PPSC), i.e. the EPCglobal Guidelines in the EPCglobal arena therefore was more or less certain from the beginning. The commitment of the actors to the EPCglobal Guidelines can be considered weak, in the sense that it lacks any formal sanction mechanism once being violated. Nevertheless, EPCglobal prescribes its members to comply with the EPCglobal Guidelines; otherwise, they may lose the EPC technology license.

Between 2005 and February 2008, we saw the German voluntary three-staged industry self-regulation initiative between private and public stakeholders for a code of conduct for the EPC industry in Germany. The industry self-regulation initiative builds upon the EPCglobal Guidelines and the ‘Recommendation on RFID’ of the ‘Düsseldorfer Kreis’ of 8/9 November 2006. The mode of governance that best described the structure and interactions of the actors in the three-staged self-regulation initiative arena is the ‘negotiation’ structure. Heterogeneous

public and private stakeholders with different perspectives and motives negotiated as equal partners in the self-regulation initiative with the aim of reaching a code of conduct for the EPC industry in Germany. The actors pursued their own individual interest and were willing to come to an accord by mutually adjust to each other. The negotiations almost reached a satisfactory agreement that would coordinate the actions of the contesting heterogeneous stakeholders accordingly. The negotiations deadlocked and were put on hold, underlining that the outcome of the policy-making in the three-staged self-regulation initiative arena was uncertain. We also saw that FoeBuD, the Informationsforum RFID, and the Federal Consumer Center employed the ‘exit option’ during the negotiations. When an agreement would have been reached, the commitment of the actors to the policy outcome for a code of conduct would have been weak, as there was not defined a formal sanction mechanism. Nevertheless, the press could have functioned as a powerful informal sanction mechanism for the EPC industry to keep the code of conduct. As the negotiations were set on hold the ‘Report German Government on RFID regulation’ of 23 January 2008 indicated that the solution to the contesting issues needed to come from the EC.

Since 2005, the OECD has been working on an RFID-specific policy recommendation that culminated in the ‘OECD Policy Guidance on RFID’ adopted on 17 June 2008. The OECD provides high-level RFID-specific policy guidance for the governments, businesses, and citizens of the OECD member countries. The mode of governance that best describes the structure and interactions of the actors in the OECD arena is a mix between ‘hierarchy and network’. The OECD as the moderating authority orchestrated the RFID-specific public debates between actors from the private sector, government, and civil society (NGOs) of the OECD member countries. The public debates took place in a more or less symmetric fashion amongst heterogeneous actors, creating a kind of policy community for collective learning. The subsequent policy outcome was more or less certain, although it took some time to reach a consensus. The commitment to the policies is rather weak, as there is no formal sanction mechanisms defined. The ‘OECD Policy Guidance on RFID’ therefore is considered a *best practice* for providing high-level policy guidance for devising RFID-specific regulation.

There are also RFID-specific harmonization initiatives between the EU and the US within the context of the ‘TEC RFID Lighthouse Priority Project’ instituted by the EU-US Summit Declaration of 30 April 2007. The governance mode that best describes the structure and interaction of the actors in this arena is also a mix between ‘hierarchy and network’. On a par with the OECD arena the EU-US arena is geared towards RFID-specific policy learning in public debates between actors from the private sector, government, and civil society, creating a policy community based upon trust and mutual adjustments. The policy outcomes therefore are certain and the commitment to the policies by the actors is weak because the outcomes are not binding by any formal authority or a formal sanction mechanism.

Since 2005 within the i2010 ICT policy framework, the EC is working on RFID-specific regulation. The activities of the EC were crystallized in the *draft* version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’ of 21 February 2008. All the previously discussed RFID-specific regulatory initiatives will come together in the *final* version of the ‘RFID Privacy, Data Protection and Security Recommendation’. Differently put, the EC can be called a ‘hub’ in connecting all the other policy-making arenas. The EC has true legislative power to make legally binding RFID-specific regulation, i.e. the ability to make a legal instrument that the EU Member States need to implement in their National legislation. The mode of governance that best describes the structure and interactions of the actors in the EC arena is a mix between ‘hierarchy and negotiations’, i.e. ‘negotiations in the administrative implementation of laws (co-operative administration).’ Hierarchical coordination and control is typical for many formal organizations and the EC is no exception. The EC takes a leadership role amongst the contesting European actors from government,

business, and civil society that take part in the policy-making processes orchestrated by the EC. The EC is the top-moderator and includes all the relevant stakeholders that have mixed motives (egoistic and cooperative orientations) and perspectives to participate in a symmetrical fashion with the aim of collective learning and finding agreement in the RFID-specific public debates. The outcome of the institutionalized negotiations in the EC policy-making arena is uncertain. Not surprisingly therefore, we see that the EC keeps postponing the publication of the final version of the ‘RFID Privacy, Data Protection and Security Recommendation’. However, once the *final* version of the ‘RFID Privacy, Data Protection and Security Recommendation’ is in place, the commitment of the actors to the outcome will be strong as it is backed up by the EC as a formal authority and potentially future European legal sanction mechanisms.

6.2 The socio-technical transformation pathway (Q5)

6.2.1 Fitting the profile

The observed empirical patterns of the RFID governance case study, described in the previous two chapters, resemble the ‘transformation pathway’, one of the five socio-technical transition pathways defined by Geels and Schot (2007a). The transition pathway is characterized by ‘moderate landscape pressure (‘disruptive change’) at a moment when niche-innovations have *not* yet been sufficiently developed, then regime actors will respond *by modifying the direction* of development paths and innovations activities’ (Geels & Schot, 2007a: 406). Figure 26 below depicts the graphical representation of the ‘transformation pathway’, in the context of the Multi-Level Perspective (MLP) on socio-technical transition as discussed in chapter two.

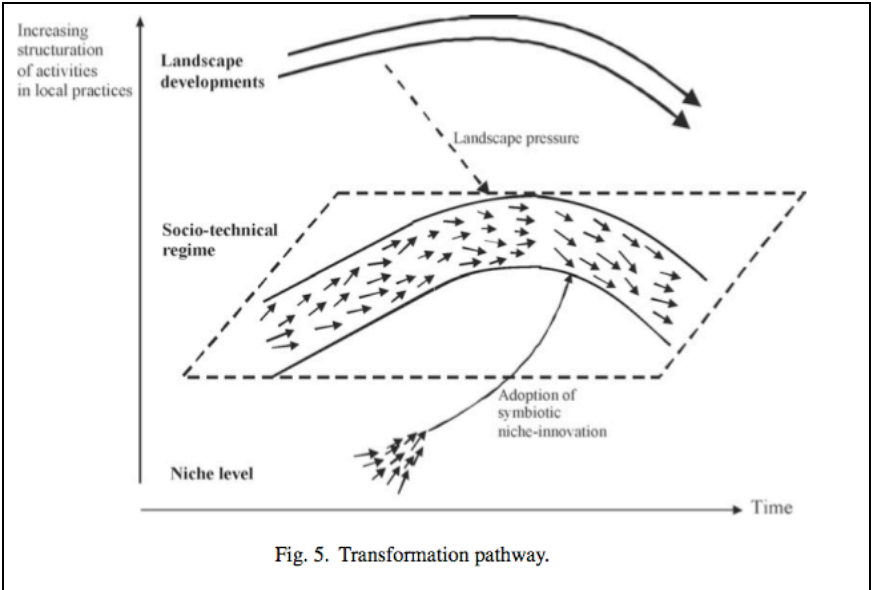


Figure 26 - Transformation pathway (Geels & Schot, 2007a: 407)

The RFID governance case study showed that the *socio-technical landscape* pressures upon the *incumbent traditional barcode regime (GSI-EAN/UPC)* and the RFID pilot projects in the *RFID technological niche (GSI-EPCglobal-EPC)* are predominantly economic in nature. The socio-technical regime and the technological niche experience regular and low intensity pressure from the socio-technical landscape. The pressure calls for a gradual change for boosting efficiency and producing more competitively in the European retail sector. The aim is to strengthen the economical position of the European retail sector in the ever-increasing

competitive global economy. Furthermore, the *RFID technological niche* grows out of the *incumbent traditional barcode regime*. The EPC industry puts forth the EPC technology as the competence-enhancer add-on or symbiotic successor to the incumbent barcode technology. The EPC technology enables to boost efficiency and to increase economic revenues in the retail value chain, i.e. boost performance and competitive prices.

In 2003, the METRO Group Future Store Initiative (MGFSI) in their ‘METRO 1’ RFID pilot project in the RFID technological niche started experimenting with the EPC technology to boost efficiency in the retail value chain. The MGFSI set out to *learn* how to *use* and *produce* the EPC technology on consumer products in the retail sector. Initially the MGFSI did not pay any attention to how to *regulate* the EPC technology applied on consumer products; hence, ‘METRO 1’ implemented no RFID-specific consumer privacy regulations. This proved to be a big mistake and triggered a consumer privacy controversy that was revealed by the consumer privacy NGOs FoeBuD and CASPIAN using the press. The criticism voiced by these societal consumer interest groups about the risks of RFID for consumer privacy marked the *wakeup call* for the EPC industry, the established consumer protection authorities, and the established governmental regulatory bodies. The bad press and the RFID Position Statement released by the consumer privacy NGOs (societal pressure groups) concerning RFID articulated the consumer privacy concerns of RFID and put it on the policy agenda. In other words, regime outsiders put pressure on the regime insiders to reorient themselves and to adjust their course of action accordingly.

The RFID governance case study showed that a multi-actor and multi-tier governance regime for consumer privacy protection of RFID for the European retail sector emerged. The governance regime consists out of the socio-technical regime insiders (technology users, producers and regulators) and the socio-technical regime outsiders (societal pressure groups); the EPC technology users and producers, the established consumer interest and protection organizations, governmental regulatory bodies, and the consumer interest NGOs. Together the contesting regime insiders and regime outsiders engaged in negotiations to gradually adjust the regime rules and in particular the RFID-specific consumer privacy regulations to accommodate RFID. These are the so-called socio-institutional dynamics between regime insiders and regime outsiders.

The RFID-specific regulatory outcomes of this emerging governance regime were a buildup from normative (behavioral) rules to regulative (formal) rules. The first RFID-specific regulatory outcome was the voluntary industry self-regulation initiative of EPCglobal that yielded a code of conduct for the EPC industry (normative rules). The German three-staged voluntary industry self-regulation also aimed at a code of conduct for the EPC industry in Germany (normative rules). The ‘OECD Policy Guidance on RFID’ contains normative guiding principles for the formulation of RFID-specific regulations (normative rules). Eventually, all these regulatory outcomes converge to codified formal regulation that enables and constrains and thus coordinates and controls the interaction amongst the contesting stakeholders (regulative rules). The key all-encompassing regulatory outcome of RFID-specific regulation will be the final version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’. The emerged RFID-specific consumer privacy regulations are imposed upon and implemented in the recently launched RFID pilot projects of ‘METRO 2’ in the RFID technological niche. As a result, there are no consumer privacy issues, however the ‘opt-in vs. opt-out’ issue is still an open issue.

In conclusion, the RFID pilot projects of the MGFSI play a key role in the ‘*policy learning process*’ amongst the regime insiders (EPC technology users and producers, and regulators) and the regime outsiders (consumer interest NGOs). These negotiations yielded RFID-specific regulation to accommodate the rollout of RFID on consumer products in the B2C application domain in the European retail sector. Therefore, the consumer privacy

controversy of ‘METRO 1’ is not a failure. Actually, it can be considered a success, as it was a key factor in stimulating the ‘collective policy learning process’ of the emerging governance regime for consumer privacy protection. The emerged governance regime is still important for the further diffusion of RFID in the retail sector, as it needs to resolve the ‘opt-in vs. opt-out’ issue, to put RFID on consumer products in the European retail sector to work.

6.2.2 Outlook based upon the transformation pathway

According to figure 26 of the ‘transformation pathway’, when we follow the trend indicated, the regime transition from the *incumbent traditional barcode regime (GSI-EAN/UPC)* to the *RFID regime (GSI-EPCglobal-EPC)*, as the result of a successful symbiotic technological niche innovation in the B2C application domain in the European retail sector, will take place. This implies that the ‘opt-in vs. opt-out’ issue is going to be resolved. Nevertheless, the question remains, when can we expect the regime transition to take place? Well, in order to say something sensible about that we need to examine the stability of the rules of how to *use*, *produce*, and *regulate* RFID in the technological niche.

We saw that between 2003 and 2008 in the technological niche, between ‘METRO 1’ and ‘METRO 2’, the MGFSI *learned* how to *use* and *produce* RFID on consumer products. The regime actors (technology users and producers) managed to globally standardize how to *use* and *produce* the EPC technology for consumer products. From the first RFID tags without proper deactivation possibilities in ‘METRO 1’, to the fully implemented EPC standards suite with the EPC Gen. 2 RFID tags that can be easily deactivated in ‘METRO 2’. Differently put, the regime actors managed to adjust the EPC technology to make a better ‘fit’ with its societal selection environment. However, the costs of the EPC infrastructure are still too high for a full-blown rollout in the retail value chain and in particular on consumer products. In order to be profitable the whole retail value chain, B2B and B2C, needs to install the EPC infrastructure, just as it is with the EAN/UPC barcode infrastructure of today. Because of the huge investments this requires, the adoption of the EPC infrastructure in the retail value chain is a slow and evolutionary process not without problems. For instance, the EPC infrastructure might prove to be too expensive for Small and Medium Enterprises (SME). Once the EPC technology manages to break through, it is expected that the first EPC tagged consumer products will become visible on the higher margin consumer products such as apparel. Once this has become profitable, the lower margin consumer products in the supermarket will be provided with the EPC tags.

We also saw that between 2005 and 2008, the MGFSI being part of the emerging multi-tier and multi-actor governance regime for protecting consumer privacy, *learned* how to *regulate* the application of RFID on consumer products. Although the emerging regulatory capability has caught up with the technology developments, it is still not enough for the further diffusion of RFID on consumer products, i.e. replacing the incumbent barcode regime. The regime actors and the outside groups are still figuring out how to regulate the EPC technology. The regulatory framework still needs to resolve the ‘opt-in vs. opt-out’ issue, to cultivate consumers’ acceptance of the EPC technology. Nevertheless, accompanying the *technological standardization* of the EPC technology, we clearly see initiatives of the EC to *harmonize* the RFID-specific regulatory framework among its Member States. In addition, also within the context of the EU-US Summit Declaration of 2007 and the OECD we see transatlantic EU-US *harmonization* initiatives for RFID-specific regulation. The dominant socially constructed policy artifact will be the final version of the EC ‘RFID Privacy, Data Protection and Security Recommendation’.

In conclusion, the socio-technical landscape pressures definitely opened up the ‘window of opportunity’ for RFID to break through. However, the (inter)actions of the socio-technical regime actors and the outside pressure groups (regime insiders and regime outsiders)

who act out the transformation pathway, have not managed to stabilize the rules of how to *use*, *produce*, and *regulate* RFID in the technological niche yet. Some rules are still under construction and more cumulative adjustments and reorientations are required (Geels & Schot, 2007a). Stable rules are needed for the breakthrough of RFID from the technological niche to the mainstream market and to grow into the new socio-technical regime. In the niche-accumulation process, RFID/EPC has definitely gained momentum in the technological niche, but not enough to become a market niche to replacing the incumbent regime yet. From a technological perspective, the EPC standards suite is definitely the standard or dominant design for how to *use* and *produce* RFID for the application on consumer products. Whereas the EPC standards suite is still too expensive for consumer products in the B2C application domain, it is already profitable in the B2B application domain on pallets and crates. From a regulatory perspective, a standard is in the making, in the embodiment of the final EC 'RFID Privacy, Data Protection and Security Recommendation'. The EC Recommendation needs to resolve the 'opt-in vs. opt-out' issue of RFID to create the envisioned stable environment for consumers to trust RFID and business to invest in RFID. Once the EPC industry and the consumer interest organizations receive the final version of the EC Recommendation well, the conditions are set for RFID to flourish on consumer products in the B2C application domain. Then RFID can grow from the technological niche to the market niche and eventually replace the barcode regime, i.e. then there will be a 'window of opportunity' and 'multi-level alignment'. Hence, as often is the case adequate regulation for technological innovation is a key-enabling factor. In the case of RFID, adequate regulation can still make or break the application of RFID on consumer products in the B2C application domain in the European retail sector.

6.3 Policy recommendation (Q6)

On the 12th of May 2009, the EC happened to publish the final version of the 'Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification' (EC-Rec-1, 2009; EC-Rec-2, 2009). Instead of formulating a policy recommendation for the 'opt-in vs. opt-out' issue in the European retail sector, section 6.3.1 will examine what the final version of the EC Recommendation on RFID says about the 'opt-in vs. opt-out' issue. Then section 6.3.2 will reflect upon these findings, in the light of the outlook about the transformation pathway as discussed in the previous section.

6.3.1 The final EC Recommendation on RFID and the 'opt-in vs. opt-out' issue

The EC is aware of the fact that the RFID technology is still in an immature stage (EC-Rec-1, 2009; EC-Rec-2, 2009). The EC therefore puts forth the Recommendation on RFID as a 'soft legal instrument' that offers more flexibility, is faster to implement, and is more cost-effective as opposed to a 'hard legal instrument' such as the Data Protection Directive. Instead of extending existing legislation, the EC Recommendation on RFID provides interpretation and guidance to the Data Protection Directive on the specific cases with RFID. In other words, the EC Recommendation on RFID states how the general rules as laid down in the technology-neutral Data Protection Directive should be applied to RFID applications. The EC Recommendation on RFID is to be transposed into the National regulations of the 27 EU Member States to create a uniform RFID-specific regulatory framework in the EU.

The EC Recommendation on RFID among other application domains aims at providing guidance to warrant consumer privacy and the processing of personal data in RFID applications in the retail sector. This as RFID has the potential to maliciously process directly or indirectly personal identifiable data of a natural person, e.g. by tracking their movements or collecting data on their purchases. To counter this, the EC Recommendation on RFID advises

a fully transparent use of RFID including clear indication of the presence of RFID tags on or embedded into consumer products (points 7-8).

Concerning the ‘opt-out vs. opt-in’ issue the EC Recommendation on RFID takes a proactive approach, by proposing the implementation of the ‘flexible opt-in principle’ (points 9-14). This entails that by means of a ‘privacy impact and data protection assessment’ (points 4-5) on a case-by-case basis needs to be assessed whether RFID tags on consumer products need to be deactivated conform the ‘opt-in principle’ or via the ‘opt-out principle’. In other words, whether the retailer needs to deactivate the tag immediately at the point of sale, or that the consumers themselves are responsible for the deactivation of the tags at the point of sale or beyond. The assessment needs to be conducted by the National data protection authority before the deployment of the RFID application. When the assessment shows that there is a risk to customer’s privacy or personal data, the RFID applications needs to make sure that RFID tags are deactivated or removed at the point of sale immediately and free of charge for the customers, i.e. in accord with the ‘opt-in principle’. In addition, consumers should be able to verify that the RFID tags are deactivated. When the assessment shows that there is no customer’s privacy or personal data risks then the RFID application is allowed to implement the ‘opt-out principle’, provided that the RFID application offers consumers free of charge and easy means to deactivate the RFID tags at the point of sale or at a later stage.

With the ‘flexible opt-in principle’, the EC aims to strike a balance between the costs for the RFID industry (including retailers) to install equipment to deactivate RFID tags immediately at the point of sale, and the acceptance of consumers to do it themselves. When the assessment shows that there is no risk for consumer privacy and personal data, retailers are allowed to implement the ‘opt-out principle’ and do not have to install deactivators at every point of sale. Nevertheless, the EC Recommendation on RFID itself calls for its monitoring and evaluation during the next two years to keep up with the technological and market developments. In addition, the EU Member States need to update the EC about the effectiveness of the EC Recommendation on RFID. Consequently, the EC can decide whether there will be a need for developing more hard and legally binding legislation in the future when the RFID technology matures.

The first reactions to the EC Recommendation on RFID by EPCglobal Europe, the Informationsforum RFID (representing EPC industry in Germany) and the European Consumers’ Organization BEUC were positive (Wessel, 2009). It seems that the final version of the EC Recommendation on RFID has resolved the ‘opt-in vs. opt-out’ issue, at least for the time being. The EC Recommendation on RFID creates a ‘level playing field’ as it were. The Recommendation on RFID warrants consumer privacy and encourages consumers to have trust in RFID, and businesses to invest in RFID applications; it therefore stimulates the further rollout of RFID applications in the European retail sector.

6.3.2 Supporting the outlook

The emerging regulatory capability for RFID seemed to have solved the opt-in vs. opt-out’ issue. It seems that solid regulation is going to ‘make’ the application of RFID on consumer product in the B2C application domain in the European retail sector. In other words, there seems to be ‘multi-level alignment’ and a ‘window of opportunity’ for RFID in the technological niche to grow into a market niche in the niche accumulation process, and complete the transformation pathway from the traditional barcode regime (GS1-EAN/UPC) to the RFID regime (GS1-EPCglobal-EPC). Currently, there are dynamically stable rules of how to *use*, *produce*, and *regulate* RFID in the B2C application domain on consumer products in the European retail sector. The dominant technological standard is the EPC standards suite based upon the EPC Gen. 2 standard, and the dominant regulatory standard is the final version of the EC Recommendation on RFID. Nevertheless, whether the full transformation pathway

will be completed eventually still needs to be seen in the near future as RFID is still on pilot level in the technological niche. Additional to future privacy issues there may pop up other issues in the innovation process. Examples could be environmental issues related to the disposal of RFID tags into the environment, health issues in relation to radiation, and radio frequency band management issues. At least for now, the EC Recommendation on RFID as an additional empirical finding endorses the outlook formulated in line with the socio-technical transformation pathway in section 6.2.2 above.

6.4 Conceptual contributions (Q7)

6.4.1 The policy niche

The RFID governance case study showed the presence of an ‘emerging multi-tier and multi-actor governance regime for consumer privacy protection that yields RFID-specific consumer privacy regulations that are imposed upon and consequently manifested in the local practices of the RFID pilot projects undertaken by the MGFSI in the technological niche. These RFID-specific regulations are developed against the backdrop of the multi-tier technology-neutral consumer privacy legislations.’ This ‘mouthful’ is what I would like to conceptualize by the *policy niche*. In doing so and by taking the RFID context out of the equation, the *policy niche* in general is defined as ‘the emerging multi-tier and multi-actor governance regime that yields technology-specific regulations to accommodate a technological innovation that is manifested in pilot projects in local practices in the technological niche.’

In this study, the *policy niche* enabled to demystify the regulatory dimension in the transformation pathway of the MLP. The *policy niche* enabled to get insights into how regulatory artifacts emerge to accommodate technological innovation in pilot projects in the technological niche. In other words, the *policy niche* enables to get insights into the social construction (processes) of policy artifacts (outcomes). These policy artifacts are developed alongside technological innovation in local pilot projects in the technological niche, to accommodate its societal embedding. The *locus* of the *policy niche* therefore is in the ‘socio-technical regime--technological niche’ interaction, qua the emerging regulatory capability for the technological niche innovation. In addition, the *policy niche* incorporates the outside societal pressure groups as well, focusing on both socio-technical regime insiders (technology users, producers, and regulators) and socio-technical regime outsiders (societal pressure groups).

In conclusion, this study showed that the pilot projects in the technological niche triggered the need for the development of policy in the *policy niche* to accommodate the technological niche innovation. The pilot projects therefore are important process variables that affect policy outcomes of the *policy niche* that in turn affect the development and diffusion of the technology being piloted in the technological niche.

6.4.2 The hybrid MLP-GP analytical framework

In this study, the conceptual contributions and refinements are as follows. Firstly, this study symbiotically integrated the Multi-Level Perspective (MLP) and the Governance Perspective (GP), hitherto two separate conceptual frameworks, into one hybrid MLP-GP analytical framework to research the regulatory dimension of socio-technical transition. More specifically, the GP served to open the ‘black box’ of the emerging regulation in socio-technical transition conceptualized by the MLP. Secondly, this study applied the hybrid MLP-GP analytical framework to the complexity and messiness of a contemporary empirical research field. This study experimentally conducted a case study of a ‘moving target’ within the empirical research field with the aim of making sense of it. As a result, the case study provided reflexivity to the empirical research field by identifying the relevant policy processes and policy outcomes in terms of the involved organizations, their perspective, their interactions, and the salient policy issues on the agenda. Thirdly, this study fed back the observed empirical patterns to the hybrid MLP-GP analytical framework. This enabled to employ the hybrid MLP-GP framework in a ‘prospective fashion’, by making an assessment about the near future socio-technical transition pathway. Consequently, this study contributed to the understanding of the ‘transformation pathway’, as one the five established socio-technical transition pathways of the MLP defined by Geels and Schot (2007a). Finally, this study developed the concept of a *policy niche* and its role in understanding the regulatory dimension in socio-technical transition. Therefore, the hybrid MLP-GP analytical framework proved to be a fruitful symbiotic framework for conducting empirical research and gaining deeper insights in the emerging regulatory capability to accommodate an emerging technology.

7. Philosophical reflection – Surveillance and privacy protection of RFID

This chapter presents a philosophical reflection upon privacy and surveillance concerning RFID. The aim is to get a more profound understanding of RFID and its privacy implications as discussed in the previous chapters. This chapter will position the subject matter in the philosophical discourse that has a more long-term perspective on technological developments and their impact upon human society in terms of privacy and surveillance. Section 7.1 sketches the broad context in which we could view RFID and its privacy implications. Section 7.2 examines more closely the link between surveillance and the violation of informational privacy. Section 7.3 subsequently examines how RFID changes the nature of surveillance. Finally, section 7.4 connects the reflections back to the findings of the RFID governance case study as presented in the previous chapters.

7.1 The advanced global information society

The investigation starts around the turn of the 19th century, when Henry Ford installed the conveyor belt assembly line to mass-produce his famous Ford T-model motorcar (Lewchuk, 1993). This era is characterized by the *Industrial age*, because it primarily dealt with the generation and distribution of energy and physical commodities. In this period, the *high-speed transportation technologies*, such as the motorcar, railroad, and air travel boomed. During the course of the 20th century, these have been seamlessly integrated with the *high-speed Information and Communication Technologies* (ICTs) such as the radio, telephone, television, personal computer, cell-phone, and the Internet. The *high-speed transportation technologies* in tandem with the *high-speed ICTs* enable a global integrated world in which people, goods, and information can easily find their way around the globe. The current status quo therefore is characterized by the phenomenon that is called *globalization* (Scheuerman, 2006). Being centered on the Internet, the contemporary ‘anywhere’ and ‘anytime’ globalized society is characterized as the network, information, or knowledge society in which information has increasingly become the ‘raw’ material. The contemporary global information society has its impact on the economical, political, social, cultural, ecological, legal, and technological dimensions of human existence (Castells, 1996; Stalder, 1998). As the current global information society primarily deals with the generation and distribution of information we can say that (western) human civilization made its entrance into the *Information Age*.

Recent innovations in wireless networking ICTs such as WiFi, 3G, Bluetooth, and RFID allow for further changes in the contemporary global information society. These wireless ICTs, especially RFID, allow the physical world of objects to be integrated with the virtual world of the Internet. This is the vision of the Internet of Things (IoT) that aims at taking the Internet to the next level. The role of RFID within the vision of the IoT falls within the overall vision of ‘Ambient Intelligence’ (AmI) (Srivastava, 2007; Floridi, 2007; Wasieleski & Gal-Or, 2008; Brey, 2005a). According to Brey (2005a), AmI is a combination of Ubiquitous Computing (UC) or Pervasive Computing (PC) and Intelligent User Interfaces (IUIs). Brey (2005a: 157) defines AmI as ‘a new paradigm in information technology that envisions a future society in which people will live and work in environments that recognize and respond to them in intelligent ways.’ Brey (2005a) argues that the key properties of AmI are its: ubiquity, invisibility, sensing, memory amplification, user profiling (recording and adapting to user behavior patterns), and connectedness (wireless communication between smart objects). AmI therefore is the major building block in what can be called the ‘advanced global information society’ (Brey, 2005a: 158). However, Brey (2005a) also argues that the properties of AmI enable the creation of detailed profiles of ones behavior, mental states, and

social interactions. As this personal information is prone to become publicly available, Aml harbors an unprecedented threat to privacy that needs to be addressed in technological development and in social policy.

RFID indeed plays a pivotal role in the transition from the global information society that is centered on the Internet, to the advanced global information society that is centered on the Internet of Things (IoT). Namely, RFID enables physical entities to become ‘smart’ and to be embedded in ‘smart networked surroundings’. Consequently, RFID allows the ‘anywhere’ and ‘anytime’ (ubiquitous) identification, authentication, tracing, and tracking of people, animals, and (consumer) objects. Despite the benefits of RFID in for instance inventory management in the retail sector, RFID poses a threat to personal privacy, as it can be associated with personal information (Lockton & Rosenberg, 2005). RFID tags on consumer products can act as personal identifiers. In this way, RFID can be employed for consumer surveillance in retail stores and beyond. For instance, by covertly tracking customers’ movements and expanding personal marketing based upon aggregated consumer preference profiles. In this way RFID has the potential to compromise consumers’ informational privacy.

In conclusion, there seems to be a link between surveillance and its threat to violating one’s informational privacy. The next section will explore in more detail how surveillance has the potential to compromise one’s informational privacy.

7.2 Informational privacy and surveillance

Within the field of philosophy, scholars debate about the meaning of the concept of ‘privacy’ (DeCew, 2008) and in particular within the field of ethics of information technology (Bynum, 2008). Within the latter field, Brey (2005b) articulates a succinct and almost intuitive definition of privacy. According to Brey (2005b: 183), privacy as a *condition* is defined as a ‘state in which others have limited access to one’s personal affairs, including personal information, the intimacies of one’s life, one’s thoughts and one’s body.’ Subsequently, privacy as a *right* is defined as ‘the right to control access to such personal affairs’ (Brey 2005b: 183).

In the last couple of decades, computers and the Internet (computer networks) enabled to easily collect (store), process (search, compare, retrieve), and exchange (share) personal information. The meaning of privacy in relation to ICTs therefore predominantly concerns informational privacy. For instance, Floridi (2005) who presents a theory of informational privacy conceives individuals to be constituted by their personal information and the processing thereof. Floridi perceives ICTs to be agents that can decrease or protect informational privacy by inducing changes in the space of information in what he calls the ‘infosphere’. Consequently, if ICTs threaten or compromise ones informational privacy, ones personal identity has been either. This conception of informational privacy resonates with the definition of Wasieleski and Gal-Or (2008: 31), who define privacy as ‘the maintenance and preservation of the integrity of an individual’s personal information and space.’ Drawing upon the definition of privacy of Brey (2005b), informational privacy then can be considered the *condition* in which others have limited access to ones personal information (information/data about oneself) and the *right* to control access to ones personal information.

According to Brey (2007), the threat to an individual’s right to informational privacy in the information society has its origin in the interest of governments and corporate entities in surveillance. Surveillance is defined as ‘the systemic monitoring (observation and data collection) of (groups) of people for specific purposes, usually with the aim of exerting some form of influence over them or managing them’ (Brey, 2007: 29; Brey 2005b: 183). Modern surveillance systems, such as video surveillance are digital (ICT-enabled) and are characterized by a distinction between the surveyor and the surveyed. This offers the possibility for surveillance of the surveyed or the data-subject to take place without explicit

'informed consent'. Consequently, ICTs have the potential to make *customer or citizen surveillance* in terms of their *personal data surveillance* by governments and large corporations an easy and covert process. Surveillance therefore has the potential to compromise one's informational privacy because its very purpose is to collect personal information to exert influence on the data-subject. Not surprisingly, that the current state of affairs have been portrayed along the lines of the George Orwell's '1984', i.e. a dystopian view of *ubiquitous surveillance* in a 'Big Brother' like society.

In conclusion, surveillance by means of ICTs has the potential to compromise one's informational privacy because of its inherent intention to do so and the ease of covertly going about it. The next section will explore how RFID changes the nature of surveillance and recommends how one's informational privacy can be protected.

7.3 RFID changes the nature of surveillance

Van den Hoven and Vermaas (2007) discuss the protection of informational privacy in relation to ubiquitous surveillance by emerging ICTs. Their argument is that emerging ICTs and especially RFID give rise to new kinds of privacy issues that need to be addressed with adequate privacy protection measures accordingly.

Van den Hoven and Vermaas (2007: 290) characterize the traditional state of affairs concerning the threat of surveillance in terms of 'panopticism'. Panopticism derives its meaning from Jeremy Bentham's 'Panopticon' that is a dome-like prison in which the inmates are constantly surveyed from a central observatory. Panopticism then is the centralized form of surveillance, monitoring, and power conform the dystopian 'Big Brother' perspective. This form of ubiquitous surveillance has the potential to harm the observed in terms of exploitation, taking advantage of them, discrimination against them, and imposing identities on them from an authoritarian standpoint. In order to counter these potential harms of panopticism, Van den Hoven and Vermaas (2007: 290) observe that the traditional view on warranting privacy of persons is primarily about the content and the processing of information about those persons. Privacy protection then is the protection of the data and information of the person. This implies the appropriate constraining of the 'acquisition, processing, use, and dissemination of personal data and information.' Van den Hoven and Vermaas (2007) observe that in the EU, the privacy laws and regulations *exactly* define such constraints on the harvesting, processing, usage, storage, and exchange of personal data and information. In addition, the EU regulations are based upon the main moral principle of 'informed consent'. Consequently, before personal information/data can be processed informed consent about how the institution is planning to store, process, and exchange the personal data from the data-subject is required. As a result, the data-subject is able to voluntarily give up his right to privacy when he decides to.

According to Van den Hoven and Vermaas (2007), RFID has the potential to fundamentally change the nature of traditional surveillance. As already discussed, RFID within the context of the Internet of Things enables physical entities to become 'smart' and to be embedded in 'smart networked surroundings'. By being such an ambient technology, RFID enables a change from the continuous centralized mode of surveillance and processing of personal data in the 'societal-panopticon' (synoptic and continuous) (Van den Hoven & Vermaas, 2007: 291), to a continuous decentralized mode of surveillance and processing of personal data outside the 'societal-panopticon' (not synoptic and continuous). In other words, the threat of surveillance will still be continuous but no longer solely organized in a central fashion. Van den Hoven and Vermaas (2007) therefore propose that privacy protection regulations need to be adapted to accommodate the change from centralized to decentralized flows of personal information/data. In addition, the focus to protect personal data should also shift to the design, and the development of the data carriers (technology/artifact) themselves

before they contain personal information. Finally, to protect personal data, users should also have more control over the surveillance technology such as the RFID tags they might be carrying.

In conclusion, RFID induces a shift from a continuous centralized mode of surveillance to a continuous decentralized mode of surveillance. Accordingly, the informational privacy protection measures by means of informational privacy policies, the design of the artifact itself, and the control people have over the artifacts need to be updated to accommodate this change. The next section will make a connection to the findings of the RFID governance case study and will show that the informational privacy regulations are catching up in accommodating the shift in the mode of surveillance.

7.4 The regulatory accommodation for RFID in the new mode of surveillance

In the *Information Age*, innovations in ICTs enable a transition from the global information society, based upon the Internet, to the advanced global information society, based upon the Internet of Things. The protection of our informational privacy already posed to be a major issue in the former and as we saw in the RFID governance case study takes the debate to new heights in the latter.

The data protection legislations in the EU provide a firm regulatory framework for warranting a person's informational privacy in the 'societal-panopticon', i.e. the traditional view of the continuous and centralized mode of surveillance. With the advent of AmI as a new paradigm for ICTs and especially the role of RFID in the Internet of Things, a change is taking place that opens up the possibility of threatening and compromising a person's informational privacy outside the 'societal-panopticon' as well, i.e. the continuous and decentralized mode of surveillance. The RFID governance case study showed that the EC takes a proactive approach is examining the current technology-neutral data protection legislation in order to see whether they accommodate informational privacy threats from ICTs such as RFID in the centralized and the emerging decentralized mode of surveillance. It became clear that the technology-neutral legislations did not prove to be adequate. Consequently, the EC developed RFID-specific regulation to supplement the existing technology-neutral data protection legislation to accommodate potential informational privacy risks associated with RFID. In line with the technology-neutral legislation, the moral principle of 'informed consent' takes central stage in RFID-specific regulation as well. For instance, the 'opt-in vs. opt-out' issue is about consumers' choice for the deactivation of RFID tags based upon their informed consent.

The RFID governance case study showed that the EC has become a major player in the emerging multi-actor and multi-tier governance regime for consumer privacy protection of RFID. The EC incorporates representatives from the industry, civil society, and governments in the regulatory processes for devising RFID-specific regulation. Furthermore, in the RFID-specific regulatory process, the EC incorporates and harmonizes with RFID-specific regulatory outcomes on other tiers in the governance regime, such as the EPCglobal Guidelines and the 'OECD Policy Guidance on RFID'. The RFID-specific endeavors of the EC converged to the final version of the 'RFID Privacy, Data Protection and Security Recommendation'. The final EC Recommendation on RFID solved the salient 'opt-in vs. opt-out' issue and created a stable regulatory outcome that accommodates potential informational privacy risks associated with RFID applications in the European retail sector. In other words, it warrants consumers against the threats to their informational privacy in the centralized and decentralized mode of surveillance. The practical adequacy and stakeholder acceptance of this pivotal piece of RFID-specific regulation is vital for the further adoption of RFID on consumer products in the European retail sector in years to come.

8. Conclusion

8.1 The main findings

The objective of this study is to get a deeper understanding of the emerging regulation in the regulatory dimension of socio-technical transition that is fleshed out empirically by the regulatory processes and regulatory outcomes concerning consumer privacy protection of RFID. In order to get these deeper insights the Multi-Level Perspective (MLP) on socio-technical transition by Geels and Schot conceptualized socio-technical transition. The MLP was employed in an *experimental fashion* to a ‘moving target’, i.e. a contemporary case study. In going about this, the MLP was combined in a *symbiotic fashion* with the Governance Perspective (GP), by Kuhlmann, Edler, and Benz, into the hybrid MLP-GP analytical framework. The GP enabled to open the ‘black box’ of the emerging regulation in the regulatory dimension of socio-technical transition as conceptualized by the MLP. The GP conceptualized the emerging regulation in terms of policy processes in multi-actor (industrial, societal, science, politico-administrative) and multi-tier (local, regional, national, transnational, international) connected policy-making arenas yielding policy outcomes for collective action.

The emerging regulation was fleshed out empirically by the emerging regulation for consumer privacy protection of RFID applied on consumer products in the business-to-consumer (B2C) application domain in the European retail sector. Thereto this study applied the hybrid MLP-GP analytical perspective to the empirical field by conducting a RFID governance case study consisting of two parts. Part one of the RFID governance case study investigated the *need* for a regulatory capability to accommodate RFID applied on consumer products in the B2C domain in the European retail sector. The analysis was centered on ‘METRO 1’, the first RFID pilot project of the METRO Group Future Store Initiative (MGFSI) in the RFID technological niche (GS1-EPCglobal-EPC). In 2004, METRO 1 caused a consumer privacy controversy of RFID that triggered the need for RFID-specific regulation in the EU. The second part of the RFID governance case study investigated the *actual* emerging regulatory capability to accommodate the emerging RFID technology in the RFID pilot projects of the MGFSI in the RFID technological niche. The analysis presented the emerging governance regime that consists of multi-tier (MGFSI, Nordrhein-Westfalen, Germany, EU, EU-US transatlantic) and multi-actor (retail, industry, consumer, privacy, governmental) regulatory processes yielding regulatory outcomes. The RFID-specific regulatory outcomes for protection consumer privacy were imposed upon and implemented in ‘METRO 2’, the recently launched RFID pilot projects of the MGFSI, yielding no consumer privacy issues.

The MLP-GP hybrid analytical framework was employed in a ‘prospective fashion’ too. This study linked the observed empirical patterns of the RFID governance case study to a particular socio-technical transition pathway as defined by Geels and Schot (2007a). The observed patterns of the RFID governance case study matched with the ‘socio-technical transformation pathway’. This transition pathway is characterized by a symbiotic niche innovation that grows out of the incumbent socio-technical regime. The RFID pilot projects conducted by the MGFSI in the RFID technological niche, i.e. METRO 1 and METRO 2, grow out of the traditional barcode regime (GS1-EAN/UPC). In addition, the ‘transformation pathway’ is characterized by the socio-institutional dynamics of cooperating, competing, and contesting stakeholders (regime insiders and regime outsiders) that adjust the socio-technical regime rules; in this case the regulatory rules concerning consumer privacy protection.

The analysis concluded that there happens to be ‘multi-level alignment’ and a ‘window of opportunity’ for the RFID in the technological niche to break through and

transform the traditional barcode regime from within to the RFID regime. There happen to be dynamically stable rules for *how to use, produce, and regulate* RFID in the technological niche. The technical standard of how to use and produce RFID on consumer products in the retail sector is the ‘EPCglobal standards suite’ based upon the ‘EPC Gen. 2 standard’. The regulatory standard of how to regulate the RFID technology on consumer products is the final version of the EC ‘Recommendation on RFID’. The regulatory standard introduced the ‘flexible opt-in principle’ that provides an adequate answer to the ‘opt-in vs. opt-out’ issue, i.e. when a retailer needs to deactivate RFID tags conform the ‘opt-in principle’ or ‘opt-out principle’ at the point of sale. Therefore, the conditions are present for RFID in the technological niche to complete the ‘transformation pathway’.

The emerging regulatory capability in terms of an emerging governance regime in the ‘technological niche--socio-technical regime interaction’ in the ‘transformation pathway’ is what I conceptualized as the *policy niche*. Within the regulatory dimension of socio-technical transition, the *policy niche* enables to conceptualize and understand the emerging regulation that accommodates an emerging technology that is experimented with in pilot projects in local practices in the technological niche.

8.2 General reflection upon the RFID governance case study

In the analysis, the results of the RFID governance case study were fruitfully interpreted by the hybrid MLP-GP analytical framework. However, the results could have been better, if I had more resources at my disposal to do additional research. For example, I could have approached more organizations that participate in the emerging governance regime for consumer privacy protection in the European retail sector. Most likely, this would have resulted in a more complete and detailed account of what kind of governance dynamics are going on between all the cooperating, competing, and contesting stakeholders in the emerging governance regime.

8.3 Research recommendation for the empirical level

Regarding the empirical level, I want to make the following recommendation for further research. This study provided insights into the current salient issue with RFID being the consumer privacy issues concerning the application of RFID on consumer products in the B2C domain in the European retail sector. A potential near future issue with RFID in this application domain could be related to environmental/ecological issues. This as the current public debates increasingly focuses on the ‘green turn’, green revolution, sustainability, the footprint upon the earth, and carbon emissions etc. On the one hand, RFID could be employed in waste management as RFID embedded in products could assist in product recycling. RFID has the potential to enable complete product life cycle management from manufacturing, through product use, recycling, and back to manufacturing. On the other hand, once RFID tags are employed on consumer products on a massive scale, and they will be thrown away on a massive scale, hazardous materials that make up RFID tags, such as silicon, copper, aluminum, would enter the garbage on a massive scale. Waste management facilities then could have major difficulties with filtering these hazardous materials out of the garbage. In addition, when RFID tags are produced and employed on a massive scale, the materials that are used to fabricate the RFID tags could become scarce. As the application of RFID is still in the field test stage, I recommend more research regarding the environmental/ecological aspects of RFID when used on a massive scale.

8.4 Research recommendation for the conceptual level

Regarding the conceptual level, I want to make the following recommendations for further research. In general, more research is needed to understand the pivotal role of policy in technological innovation, i.e. emerging policy to accommodate an emerging technology. Specifically, more research is needed to investigate the role of the *policy niche* in socio-technical transition, i.e. the emerging regulatory capability to accommodate an emerging technology in pilot projects in the technological niche. Furthermore, in the RFID governance case study there happened to be a *policy niche* in the ‘transformation pathway’ as on one of the five transformation pathways as defined by Geels and Schot (2007a). Therefore, more research is needed to investigate whether policy niches can be identified in the other socio-technical transition pathways and to what extent they are relevant for the specific socio-technical transition pathway.

In conclusion, this study touched upon the complexity of how regulation to accommodate an emerging technology comes into being. The story is not over yet, as the RFID technology as a promising near future information and communication technology is still on the pilot level. Hence, the further developments of the RFID technology and policies for its societal embedding remain an intriguing object for investigation, especially for studies concerning policies of technological innovation.

Acronyms

Acronym	English	German
AmI	Ambient Intelligence	
B2B	Business-to-Business	
B2C	Business-to-Consumer	
BDSG	Federal Data Protection Act	Bundesdatenschutzgesetz
BEUC	European Consumers' Organization	French: Bureau Européen des Unions de Consommateurs
BfDI	Federal Commissioner for Data Protection and Freedom of Information	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit'
BITKOM	German Association for Information Technology Telecommunications and New Media	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BMELV	Federal Ministry of Food, Agriculture and Consumer Protection	Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
BMI	Federal Ministry of the Interior	Bundesministerium des Innern
BMWi	Federal Ministry of Economics and Technology	Bundesministerium für Wirtschaft und Technologie
BRIDGE	Building Radio Frequency IDentification solutions for the Global Environment	
BSI	Federal Office for Information Security	Bundesamt für Sicherheit in der Informationstechnik
CASPIAN	Consumers Against Supermarket Privacy Invasion and Numbering	
CERP	Cluster of European RFID Projects	
CPILT	Consumer Product Item-Level Tagging	
DG FSJ	Directorate-General for Freedom Security and Justice	
DG INFSO	Directorate-General Information Society and Media	
DG Research	Directorate-General Research	
DHL	Deutsche Post World Net	
DNS	Domain Name Server	
DSG NRW	Data Protection Act NRW	Datenschutzgesetz Nordrhein-Westfalen
DSTI	Directorate for Science, Technology and Industry (OECD)	
DVD	German Association for Data Protection	Deutsche Vereinigung für Datenschutz'
EABC	European-American Business Council	
EAN	European Article Number, barcode standard in the EU issued by GS1 global	
EC	European Commission	
EDPS	European Data Protection Supervisor	
EECC	European EPC Competence Center	
EESC	European Economic and Social Committee	
EICAR	RFID task force of the European Institute for Computer Anti-Virus Research	

EPC	Electronic Product Code, global RFID standard issued by EPCglobal	
ERRT	European Retail Round Table	
ETSI	European Telecommunications Standards Institute	
EU	European Union	
FCC	Federal Communications Commission	
FoeBuD	Association for the Promotion of Public Mobile and Immobile Data Traffic	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs
FP6	Sixth Research Framework Program	
FP7	Seventh Research Framework Program	
FTC	Federal Trade Commission	
GP	Governance Perspective	
HF	High Frequency	
ICCP	Committee for Information, Computer and Communications Policy (OECD)	
ICT	Information and Communication Technology	
IML	Fraunhofer-Institute for Material Flow and Logistics	Fraunhofer-Institut für Materialfluss und Logistik
IoT	Internet of Things	
ISO	International Standardization Organization	
ITU	International Telecommunications Union	
IUI	Intelligent User Interface	
LDI-NRW	North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen'
LF	Low Frequency	
MGFSI	METRO Group Future Store Initiative	
MIT	Massachusetts institute of Technology	
MLP	Multi-Level Perspective on socio-technical transitions	
MUNLV	Ministry of the Environment and Conservation, Agriculture and Consumer Protection of the German State of North Rhine-Westphalia	Ministerium für Umwelt und Naturschutz, Landwirtschaft und Verbraucherschutz des Landes Nordhein-Westfalen'
NGO	Non Governmental Organizations	
NRW	North Rhine-Westphalia	Nordrhein Westfalen
OECD	Organization for Economic Co-operation and Development	
ONS	Object Name Server	
OoS	Out of Stocks	
PC	Pervasive Computing	
PET	Privacy Enhancing Technologies	
PFIP	Principles of Fair Information Practice	
PIA	Privacy Impact Assessment	
PN	Policy Niche	

PoS	Point of Sale	
PPAC	Public Policy Advisory Council (PPAC)	
PPSC	Public Policy Steering Committee (EPCglobal)	
RF	Radio Frequencies	
RFID	Radio Frequency Identification	
RIPSA	Research and Innovation Stakeholders' Arena	
ROI	Return On Investment	
SME	Small and Medium Enterprises	
TABD	TransAtlantic Business Dialogue	
TEC	Transatlantic Economic Council	
TKG	Telecommunications Act	Telekommunikationsgesetz
UC	Ubiquitous Computing	
UHF	Ultra High Frequency	
UPC	Universal Product Code, barcode standard in the US issued by GS1global	
US	United States	
VZ-BV	Federation of German Consumer Organizations	Verbraucherzentrale Bundesverband
VZ-NRW	Consumer Center NRW	Verbraucherzentrale NRW
WPIE	Working Party Information Economy	
WPISP	Working Party on Information Security and Privacy	

Bibliography

[Allison, 1971]

Allison, G.T. (1971), *Essence of decision: explaining the Cuban Missile Crisis*, Little, Brown & Company (Canada) Limited.

[Allison & Zelikow, 1999]

Allison G.T. and Zelikow P.D. (1999), *Essence of decision: explaining the Cuban Missile Crisis 2nd edition*, Addison-Wesley Educational Publishers Inc.

[Auto-ID, 2009]

Auto-ID labs (2009), "Homepage", URL: <http://www.autoidlabs.org/>, visited 02 April 2009.

[Bent, 2009]

Bent Systems, "RFID Applications", URL: <http://www.bentsystems.com/rfidapplications.shtml>, visited 02 April 2009.

[Benz, 2006]

Benz, A. (2006), "Governance in Connected Arenas – Political Science Analysis of coordination and Control in Complex Rule Systems", Chapter 1a, in: Jansen, D. (ed.), *New Forms of Governance in Research Organizations: From Disciplinary Theories towards Interfaces and Integration*, Heidelberg, Springer.

[Beugelsdijk, 2006]

Beugelsdijk, R. (2006), "RFID. Promising or irresponsible? Contribution to the social debate about RFID", Dutch Data Protection Authority (Dutch DPA: College Bescherming Persoonsgegevens (CBP)), The Hague, the Netherlands.

[BMW, 2006]

German Federal Ministry of Economics and Technology (BMW) (2006), "Bericht der bundersregierung – Stand der Umsetzung und Einfuhrung der RFID-Technologie in Deutschland",

URL: <http://www.bmw.de/BMW/Navigation/Technologie-und-Innovation/Informationsgesellschaft/rfid.html>.

[BMW, 2007]

German Federal Ministry of Economics and Technology (BMW) (2007), "RFID: Prospective for Germany -- The state of radio frequency identification based applications and their outlook in national and international markets", URL: <http://www.bmw.de/BMW/Redaktion/PDF/Publikationen/rfid-prospectives-for-germany.property=pdf,bereich=bmw,sprache=de,rwb=true.pdf>.

[BMW, 2008]

German Federal Ministry of Economics and Technology (BMW) (2008), "Reflection Paper of the Federal Government of Germany: From Berlin 2007 to Nice 2008 and Beyond: 'RFID-Internet of Things- Internet of the Future'", URL: http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeucommission/Reflections_on_European_Policy_Outlook_RFID.pdf.

[Brey, 2005a]

Brey, P. (2005), "Freedom and Privacy in Ambient Intelligence", *Ethics and Information Technology*, Vol. 7, No. 3, pp. 157-166.

[Brey, 2005b]

Brey, P. (2005), "Editorial introduction – Surveillance and privacy", *Ethics and Information Technology*, Vol. 7, No. 4, pp. 183-184.

[Brey, 2007]

Brey, P. (2007), "Ethical Aspects of Information Security and Privacy", in: *Security, Privacy, and Trust in Modern Data Management*, M. Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21-36.

[Bundestag, 2008]

Report Federal German Government on RFID (2008), “Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie”, URL: <http://dip21.bundestag.de/dip21/btd/15/052/1505252.pdf>.

[Bynum, 2008]

Bynum, T. (2008), “Computer Ethics: Basic Concepts and Historical Overview”, *Stanford Encyclopedia of Philosophy*, URL: <http://plato.stanford.edu/entries/ethics-computer/>, visited 29 April 2009.

[CASPIAN, 2003]

CASPIAN (2003), “Joint RFID Position Statement”, URL: http://www.spychips.com/jointrfid_position_paper.html, visited 02 April 2009.

[CASPIAN, 2004]

CASPIAN (2004), “Metro Future Store Special Report”, URL: <http://www.spychips.com/metro/overview.html>, visited 02 April 2009.

[Castells, 1996]

Castells, M. (1996), *The Rise of the Network Society: The Information Age: Economy, Society and Culture*, Blackwell Publishers Inc.

[Collins, 2004]

Collins J. (2004), “METRO Launches RFID Test Centre”, *RFID Journal*, URL: <http://www.rfidjournal.com/article/view/1019/>, visited 02 April 2009.

[DeCew, 2008]

DeCew, J. (2008), “Privacy”, *The Stanford Encyclopedia of Philosophy*, URL: <http://plato.stanford.edu/archives/fall2008/entries/privacy/>, visited 29 April 2009.

[EC, 2009]

European Commission (EC), (2009), URL: http://ec.europa.eu/index_en.htm, visited 29 April 2009.

[EC & BMWi, 2007]

European Commission Directorate-General Information Society and Media (DG INFSO) and the German Federal Ministry of Economics and Technology (BMWi) (2007), “European Policy Outlook RFID”, European Commission Brussels, URL: http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeuropacommission/European_Policy_Outlook_RFID.pdf.

[EC-CERP, 2009]

European Commission (EC) (2009), “Cluster European RFID Projects (CERP)”, URL: http://cordis.europa.eu/fp7/ict/enet/clusters_en.html and <http://www.rfid-in-action.eu/cerp>, visited 29 April 2009.

[EC-DG-FSJ, 2009]

European Commission Directorate-General for Justice, Freedom and Security (DG-JFS) (2009), URL: http://ec.europa.eu/dgs/justice_home/index_en.htm, visited 29 April 2009.

[EC-DG-INFSO, 2009]

European Commission Directorate-General Information Society and Media (DG INFSO) (2009), URL: http://ec.europa.eu/dgs/information_society/index_en.htm or http://ec.europa.eu/information_society/index_en.htm, visited 29 April 2009

[EC-DG-INFSO-Pol, 2009]

European Commission Directorate-General Information Society and Media (DG INFSO) (2009), “Policies”, URL: http://ec.europa.eu/information_society/tl/policy/index_en.htm, visited 29 April 2009.

[EC-DG-INFSO-Act, 2009]

European Commission Directorate-General Information Society and Media (DG INFSO) (2009), “Activities”, URL: http://ec.europa.eu/information_society/tl/activities/index_en.htm and http://ec.europa.eu/information_society/tl/research/index_en.htm, visited 29 April 2009.

[EC-DG-Research, 2009]

European Commission Directorate-General for Research (DG Research), URL: http://ec.europa.eu/dgs/research/index_en.html, visited 29 April 2009.

[EC-DPD, 2009]

European Commission Directorate-General for Justice, Freedom and Security (DG-JFS), “Status of implementation of Directive 95/46”, URL: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm, visited 29 April 2009.

[EC & EPoSS, 2008]

European Commission Directorate-General Information Society and Media (DG INFSO) and the European Technology Platform on Smart Systems Integration (EPoSS) (2008), “Internet of Things in 2020: A Roadmap for the Future”, URL: <http://www.smart-systems-integration.org/public/internet-of-things>.

[EC-Expert, 2009]

European Commission (EC) (2009), “RFID Expert Group”, URL: <http://ec.europa.eu/transparency/regexpert/detail.cfm?ref=2040&l=all>, visited 29 April 2009.

[EC-FP6, 2009]

European Commission (EC) (2009), “Sixth Research Framework Program (FP6)”, URL: <http://cordis.europa.eu/fp6/whatisfp6.htm>, visited 29 April 2009.

[EC-FP7, 2009]

European Commission (EC) (2009), “Seventh Research Framework Program (FP7)”, URL: http://cordis.europa.eu/fp7/home_en.html, visited 29 April 2009.

[EC-i2010-strategy-doc, 2009]

European Commission (EC), (2009), “Key policy documents of the i2010 strategy”, URL: http://ec.europa.eu/information_society/europe/i2010/key_documents/index_en.htm, visited 29 April 2009.

[EC-i2010-Lisbon, 2009]

European Commission (EC) (2009), “The i2010 strategy within the context of the Lisbon strategy”, URL: http://ec.europa.eu/information_society/europe/i2010/ict_and_lisbon/index_en.htm, visited 29 April 2009.

[EC-ICT-Research, 2009]

European Commission (EC) (2009), “EU ICT research projects”, URL: <http://cordis.europa.eu/fp7/ict/>, <http://cordis.europa.eu/ist/home.html>, visited 29 April 2009.

[EC-IoT, 2009]

European Commission Directorate-General Information Society and Media (DG INFSO), “RFID and the Internet of Things (IoT)”, URL: <http://www.iot-visitthefuture.eu/>, visited 29 April 2009.

[EC-Memo, 2008]

European Commission Press Release RAPID (2008), “Radio Frequency Identification Devices (RFID): Frequently Asked Questions”, MEMO/08/145”, URL: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/145&format=PDF&aged=1&language=EN&guiLanguage=en>.

[EC-networkRFID, 2009]

European Commission Directorate-General Information Society and Media (DG INFSO) (2009), “Race networkRFID: Positioning the EU as a world leader in RFID Excellence”, URL: <http://www.race-networkrfid.eu/>, visited 29 April 2009.

[EC-Rec-1, 2009]

European Commission (2009), “European Commission Staff Working Document accompanying the Commission Recommendation on the implementation of privacy and data protection principles supported by radio frequency identification - Summary of the Impact Assessment”, {C (2009) 3200 final} {SEC (2009) 585}, URL: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf.

[EC-Rec-2, 2009]

European Commission (2009), “European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification”, {C (2009) 3200 final} {Sec (2009) 586}, URL: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf.

[EC-RFID-Policy, 2009]

European Commission Directorate-General Information Society and Media (DG INFSO) (2009), “RFID and the Internet of Things (IoT)”, URL: http://ec.europa.eu/information_society/policy/rfid/index_en.htm, visited 29 April 2009.

[EC-Sym, 2008]

European Commission Directorate-General Information Society and Media (DG INFSO (Rebecca Schindler) (2008), “Transatlantic Symposium on the Societal Benefits of RFID”, Transatlantic Symposium Report, URL: http://ec.europa.eu/information_society/policy/rfid/documents/EUUSsymposium092008.pdf.

[EC-WP, 2009]

European Commission Directorate-General for Justice, Freedom and Security (DG-JFS), “Article 29 Data Protection Working Party”, URL: http://ec.europa.eu/justice_home/fsi/privacy/workinggroup/index_en.htm, visited 29 April 2009.

[EECC, 2009]

European EPC Competence Centre (EECC), “Homepage”, URL: <http://www.eecc.info/>, visited 02 April 2009.

[Eisenhardt, 1989]

Eisenhardt, K.M. (1989), “Building Theories form Case Study Research”, *The Academy of Management Review*, Vol. 14, No. 4, pp. 532-550.

[Eisenhardt & Graebner, 2007]

Eisenhardt, K.M. and Graebner, M.E. (2007), “Theory Building from Cases: Opportunities and Challenges”, *Academy of Management Journal*, Vol. 50, No. 1, pp. 25-32.

[EPCglobal, 2005]

EPCglobal (2005), “EPCglobal Guidelines on EPC for Consumer Products”, URL: http://www.epcglobalinc.org/public/ppsc_guide/, visited 02 April 2009.

[EPCglobal, 2009a]

EPCglobal (2009), “Board of governance”, URL: <http://www.epcglobalinc.org/about/governance/>, visited 02 April 2009.

[EPCglobal, 2009b]

EPCglobal (2009), “EPC Standards Suite”, URL: <http://www.epcglobalinc.org/standards/>, visited 02 April 2009.

[EPCglobal, 2009c]

EPCglobal (2009), “Public Policy Steering Committee (PPSC)”, URL: <http://www.epcglobalinc.org/public/>, visited 02 April 2009.

[EPCglobal, 2009d]

EPCglobal, “Homepage”, URL: <http://www.epcglobalinc.org/>, visited 02 April 2009.

[Floridi, 2005]

Floridi, L. (2005), “The Ontological Interpretation of Information Privacy”, *Ethics and Information Technology*, Vol. 7, No. 4, pp. 185-200.

[Floridi, 2007]

Floridi, L. (2007), “A look into the future impact of ICT on our lives”, *The Information Society*, Vol. 23, No. 1, pp. 59-64.

[FoeBuD, 2003]

FoeBuD (2003), “Big Brother Awards”, URL: <http://www.bigbrotherawards.de/2003/cop>, visited 02 April 2009.

[FoeBuD, 2004]

FoeBuD (2004), “Der Metro-Skandal”, URL: <http://www.foebud.org/rfid/metro/>, visited 02 April 2009.

[FTC, 2004]

Federal Trade Commission (FTC) (2004), workshop entitled: “RFID – Radio Frequency Identification: Applications and implications for Consumers”, URL: <http://www.ftc.gov/bcp/workshops/rfid/index.shtm>, visited 29 April 2009.

[FTC, 2005]

Federal Trade Commission (FTC) (Deborah Platt Majoras, Orson Swindle, Thomas B. Leary, Pamela Jones Harbour, Jon Leibowitz) (2005), “RFID Radio Frequency Identification: Applications and Implications for Consumers -- A Workshop Report from the Staff of the Federal Trade Commission”, URL: <http://www.ftc.gov/bcp/workshops/rfid/index.shtm>.

[FTC, 2008a]

Federal Trade Commission (FTC) (2008), “The U.S. Federal Trade Commission Staff Comments to the European Commission on its ‘Draft Recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID)’”, URL: <http://www.ftc.gov/oia/commentsrfid.pdf>.

[FTC, 2008b]

Federal Trade Commission (FTC) (2008), “Transatlantic RFID Workshop on Consumer Privacy and Data Security: Transcript Panel 2: Item-Level Tagging in Retail”, URL: http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/092308_sess2.pdf.

[FTC, 2008c]

Federal Trade Commission (FTC) (2008), “Transatlantic RFID Workshop on Consumer Privacy and Data Security”, URL: <http://www.ftc.gov/bcp/workshops/transatlantic/index.shtml>, visited 29 April 2009.

[Garfinkel, 2006]

Garfinkel, S. (2006), “Privacy Protection and RFID”, in: *Ubiquitous and Pervasive Commerce*, G. Roussos (ed.), Springer London, pp. 177-188.

[Geels, 2002]

Geels, F. W. (2002), “Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study”, *Research Policy*, Vol. 31, No. 8/9, pp. 1257-1274.

[Geels, 2004]

Geels, F. W. (2004), “From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory”, *Research Policy*, Vol. 33, No. 6/7, pp. 897-920.

[Geels, 2006a]

Geels, F. W. (2006), “The hygienic transition from cesspools to sewer systems (1840-1930): The dynamics of regime transformation”, *Research Policy*, Vol. 35, No. 7, pp. 1069-1082.

[Geels, 2006b]

Geels, F.W. (2006), “Multi-Level Perspective on System Innovation: Relevance for Industrial Transformation”, in: *Understanding Industrial Transformation*, X. Olsthoorn and A. J. Wiczcerek (Eds.), Springer Netherlands, pp. 163-186.

[Geels, 2007]

Geels, F.W. (2007), “Feelings of discontent and the promise of middle range theory for STS: examples from technology dynamics”, *Science, Technology and Human Values*, Vol. 32, No. 6, pp. 627-651.

[Geels & Kemp, 2007]

Geels, F.W. and Kemp, R. (2007), “Dynamics in socio-technical systems: typology of change processes and contrasting case studies”, *Technology in Society*, Vol. 29, No. 4, pp. 441-455.

[Geels & Raven, 2006]

Geels, F.W. and Raven, R.P.J.M. (2006), “Non-linearity and expectations in niche-development trajectories: ups and downs in Dutch biogas development (1973-2003)”, *Technology Analysis and Strategic Management*, Vol. 18, No. 3/4, pp. 375-392.

[Geels & Schot, 2007a]

Geels, F. W. and Schot, J. (2007), “Typology of sociotechnical transition pathways”, *Research Policy*, Vol. 36, No. 3, pp. 399-417.

[Geels & Schot, 2007b]

Geels, F.W. and Schot, J. (2007), “Niches in evolutionary theories of technical change – A critical survey of the literature”, *Journal of evolutionary economics*, Vol. 17, No. 5, pp. 605-622.

[Geels & Schot, 2008]

Schot, J.W. and Geels, F.W. (2008), “Strategic niche management and sustainable innovation journeys: theory, findings, research agenda, and policy”, *Technology Analysis & Strategic Management*, Vol. 20, No. 5, pp. 537-554.

[Genus & Coles, 2008]

Genus A. and Coles A. (2008), “Rethinking the multi-level perspective of technological transitions”, *Research Policy*, Vol. 37, No. 9, pp. 1436–1445.

[Graczewski & Man, 2006]

Graczewski T. and Man A. (2006), “Partnering for the Future: The case of the Future Store Initiative”, Alliance Science Centre, Eindhoven University, Eindhoven, The Netherlands.

[Hof & Cornelissen, 2006]

Hof van ‘t, C. and Cornelissen J. (2006), “RFID and Identity Management in Everyday Life – Case Studies on the Frontline of Developments Towards Ambient Intelligence”, Report IP/A/STOA/FWC/2005-28, Luxembourg: European Parliament.

[Hof, 2007]

Hof van ‘t, C. (2007), “RFID and Identity Management in Everyday Life – Striking the balance between convenience, choice and control”, Report IP/A/STOA/FWC/2005-28, Luxembourg: European Parliament.

[Holland-Letz, 2006]

Holland-Letz, M. (2006), “RFID: Funketiketten im Einsatz”, Documentary, Germany, URL: <http://www.politische-bildung.nrw.de/multimedia/02298/index.html>, viewed 02 April 2009.

[Van den Hoven & Vermaas, 2007]

Van den Hoven, J. and Vermaas, P.E. (2007), “Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon”, *Journal of Medicine and Philosophy*, Vol. 32, No. 3, pp. 283-297.

[Van den Hoven, 2008]

Van den Hoven, J. (2008), “The Tangled Web of Tiny Things: Privacy Implications of Nano-electronics”, in: *Nanotechnology & Society -- Current and Emerging Ethical Issues*, F. Allhoff and P. Lin (Eds.), Springer Netherlands, pp. 147-162.

[Kalyanam et al., 2006]

Kalyanam, K, Lal, R., Wolfram, G. (2006), “Future Store Technologies and Their Impact on Grocery Retailing”, in: *Retailing in the 21st Century*, Krafft M. and Mantrala, M., (Eds.), Springer: Berlin, pp. 95-112.

[Kreis, 2006]

Dusseldorfer Kreis Recommendation on RFID (2006), “Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich: Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten”, URL: <http://www.datenschutz-berlin.de/content/deutschland/duesseldorfer-kreis>.

[Kuhlmann, 2001]

Kuhlmann, S. (2001), “Future governance of innovation policy in Europe -- three scenarios”, *Research Policy*, Vol. 30, No. 6, pp. 953-976.

[Kuhlmann, 2002]

Kuhlmann, S. (2002), *Governance and Intelligence in Research and Innovation Systems*, University of Utrecht: Utrecht, The Netherlands.

[Kuhlmann, 2003]

Kuhlmann, S. (2003), “Evaluation of research and innovation policies: a discussion of trends with examples from Germany”, *International Journal of Technology Management*, Vol. 26, Nos. 2/3/4, pp. 131-149.

[Kuhlmann, 2007]

Kuhlmann, S. (2007), *Governance of Innovation: Practice, policy, and theory as dancing partners*, University of Twente: Enschede, The Netherlands.

[Kuhlmann, 2007b]

Kuhlmann, S. (2007), “Governance of Research – Nine Comments on Arthur Benz in Complex Rule Systems”, Chapter 1b, in: Jansen, D. (ed.), *New Forms of Governance in Research Organizations: From Disciplinary Theories towards Interfaces and Integration*, Heidelberg, Springer.

[Kuhlmann & Edler, 2003]

Kuhlmann, S. and Edler J. (2003), “Scenarios of technology and innovation policies in Europe: Investigating future governance”, *Technological Forecasting and Social Change*, Vol. 70, No. 7, pp. 619-637.

[Langheinrich, 2007]

Langheinrich, M. (2007), “RFID and Privacy”, in: Security, Privacy and Trust in Modern Data Management, Petkovic M. and Jonker W. (Eds), Springer Berlin Heidelberg, pp. 433-450.

[LDI-NRW, 2009]

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI-NRW) (2009), URL: <https://www.ldi.nrw.de/>, viewed 29 April 2009.

[Lewchuk, 1993]

Lewchuk, W.A. (1993), “Men and Monotony: Fraternalism as a Managerial Strategy at the Ford Motor Company”, *The Journal of Economic History*, Vol. 53, No. 4, pp. 824-856.

[Lockton & Rosenberg, 2005]

Lockton, V. and Rosenberg, R.S., (2005), “RFID: The next serious threat to privacy”, *Ethics and Information Technology*, Vol. 7, No. 4, pp. 221-231.

[Loebbecke, 2004]

Loebbecke, C. (2004), “Modernizing retailing worldwide at the point of sale”, *MIS Quarterly Executive*, Vol. 3, No. 4, pp. 177-187.

[Loebbecke, 2005]

Loebbecke, C. (2005), “RFID technology and applications in the retail supply chain: The early Metro Group pilot”, *18th Bled eConference*, Bled, Slovenia, June 6–8.

[METRO Group, 2003]

METRO Group press release (2003), “Future Store: Starting Out on the Future of Retailing”, URL: http://www.metrogroup.ro/servlet/PB/menu/1005578_12/index.htm, visited 02 April 2009.

[METRO Group, 2004]

METRO Group press release (2004), “METRO Group opens RFID Innovation Centre in Neuss”, URL: http://www.metrogroup.de/servlet/PB/menu/1011429_12/index.htm, visited 02 April 2009.

[METRO Group, 2007]

METRO Group press release (2007), “Galeria Kaufhof welcomes its customers to a new era of shopping: innovative technology makes service better than ever”, URL: <http://www.future-store.org/fsi-internet/html/en/3149/index.html>, visited 29 April 2009

[METRO Group, 2008]

METRO Group press release (2008), “METRO Group and real,- open the store of the future”, URL: <http://www.future-store.org/fsi-internet/html/en/16668/index.html>, visited 29 April 2009.

[MGFSI, 2008]

METRO Group Future Store Initiative (MGFSI) (2008), “METRO Group and RFID – Information about the new technology in trade and retailing”, information brochure available at: URL: <http://www.future-store.org>.

[MGFSI, 2009]

METRO Group Future Store Initiative (MGFSI) (2009), “Homepage”, URL: <http://www.future-store.org/fsi-internet/html/en/7551/index.html>, visited 29 April 2009.

[MGFSI, 2009b]

METRO Group Future Store Initiative (MGFSI) (2009), “The EPCglobal Guidelines implemented at the MGFSI”, URL: <http://www.future-store.org/fsi-internet/html/en/1723/index.html>, visited 29 April 2009.

[MSDN, 2006]

Microsoft Developer Network (MSDN) (2009), “Office Business Applications for Store Operations”, URL: <http://msdn.microsoft.com/en-us/library/aa905316.aspx>, visited 02 April 2009.

[NCSL, 2008]

National Conference of State Legislatures (NCSL) (2008), “State Statutes Relating to Radio Frequency Identification (RFID) and Privacy”, URL: <http://www.ncsl.org/programs/lis/privacy/rfidlaws.htm>, visited 29 April 2009.

[OECD, 1980]

OECD (1980), “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, URL: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1.00.html, visited 29 April 2009.

[OECD, 2008]

OECD (2008), “RFID Guidance and Reports”, OECD Digital Economy Papers, No. 150, OECD publishing, URL: <http://www.oecd.org/dataoecd/19/42/40892347.pdf>, visited 29 April 2009.

[RFID Journal, 2003]

RFID Journal (2003), “METRO opens ‘Store of the Future’”, URL: <http://www.rfidjournal.com/article/view/399>, visited 02 April 2009.

[RFID Journal, 2009]

RFID Journal (2009), “The History of RFID Technology”, URL: <http://www.rfidjournal.com/article/view/1338/1/129>, visited 02 April 2009.

[RFID Journal, 2009b]

RFID Journal (2009), “About RFID Journal”, URL: <http://www.rfidjournal.com/article/articleview/203>, visited 02 April 2009.

[Rip & Kemp, 1998]

Rip, A. and Kemp, R. (1998), “Technological change”, in: S. Rayner and E.L. Malone, (Eds.), *Human Choice and Climate Change*, Vol. 2, Battelle Press, Columbus, OH, pp. 327–399.

[Roberti, 2008]

Roberti, M. (2008), "An RFID Policy for the New Administration", *RFID Journal*, URL: <http://www.rfidjournal.com/article/print/4438>, visited 29 April 2009.

[Sarma, 2005]

Sarma, S. (2005), "A history of the EPC", in: *RFID: Applications Security, and Privacy*, Garfinkel, S. and Rosenberg, B., (Eds.), Addison-Wesley, Upper Saddle River, NJ, pp. 37–55.

[Scheuerman, 2006]

Scheuerman, W. (2006), "Globalization", *Stanford Encyclopedia of Philosophy*, URL: <http://plato.stanford.edu/entries/globalization/>, visited 29 April 2009.

[Srivastava, 2007]

Srivastava, L. (2007), "Radio Frequency Identification: Ubiquity for Humanity", *Info (ITU)*, Vol. 9, No.1, pp. 4-14.

[Stalder, 1998]

Stalder, F. (1998), "The Network Paradigm: Social Formations in the Age of Information", *The Information Society*, Vol. 14, No. 4, pp. 301-308.

[Summit, 2007]

EU-US Summit declaration of 30 April 2007,

URL: http://ec.europa.eu/information_society/policy/rfid/documents/lighthouse.pdf, visited 29 April 2009.

[Swedberg, 2008]

Swedberg, C. (2008), "At Metro's New Future Store, RFID Helps Assure Meat Quality", *RFID Journal*, URL: <http://www.rfidjournal.com/article/articleview/4109/1/1/>, visited 29 April 2009.

[TABD, 2008]

Transatlantic Business Dialog (TABD) (2008), "Transatlantic Symposium on the Societal Benefits of RFID", URL:

http://www.tabd.com/index.php?option=com_content&task=view&id=89&Itemid=99, visited 29 April 2009.

[Thiesse, 2007]

Thiesse, F. (2007), "RFID, privacy and the perception of risk: A strategic framework", *The Journal of Strategic Information Systems*, Vol. 16, No. 2, pp. 214-232.

[Wasieleski & Gal-Or, 2008]

Wasieleski, D.M. and Gal-Or, M. (2008), "An enquiry into the ethical efficacy of the use of radio frequency identification technology", *Ethics and Information Technology*, Vol. 10, No. 1, pp. 27-40.

[Wessel, 2007]

Wessel, R. (2007), "Metro Group's Galeria Kaufhof Launches UHF Item-Level Pilot", *RFID Journal*, URL: <http://www.rfidjournal.com/article/view/3624/3>, visited 29 April 2009.

[Wessel, 2009]

Wessel, R. (2009), "European Commission Issues RFID Privacy Recommendation", *RFID Journal*, URL: <http://www.rfidjournal.com/article/view/4890/>, visited 18 May 2009.

Appendices

Appendix A – The Interview Protocol

Introduction

Currently I am undertaking a research project regarding the Radio Frequency IDentification (RFID) technology. This within the context of my Master Thesis in the field of Science, Technology, Policy and Innovation studies at the University of Twente located in Enschede in the Netherlands. The focus of my research is the emerging application of the RFID technology in the retail sector on individual consumer products (product-level item tagging). What I am interested in is what this new application domain of the RFID technology, in respect to the barcode, entails for the retail sector in the near future. Next to the theoretical components of my research I want to analyze a real-life pilot project in which experiments are being undertaken with the RFID technology in its in-store product-level application domain. Next August until December, as the second part of my Master Thesis I will visit the school of public policy of Georgia Tech University located in Atlanta in the United States. Therefore, I would like to investigate one pilot project case in the EU and one in the US in order to see what the striking similarities and differences are. As a RFID pilot project for the EU I have selected the METRO Group Future Store Initiative (see <http://www.future-store.org/fsi-internet/html/en/375/index.html>) in which several experiments are being undertaken with RFID in a real-life context on product-level item tagging in the retail sector. For instance, the Galeria Kaufhof-METRO-Gardeur RFID project in Essen (see <http://www.future-store.org/fsi-internet/html/en/1613/index.html>) and since recently the Real Future Store in Toenistorst (see <http://www.future-store.org/fsi-internet/html/en/7524/index.html>).

Formalities

Date:

Organization:

Location:

Permission to record interview:

Name interviewee:

Educational background interviewee:

The role or function of the interviewee within the organization:

Period of the interviewee being employed at the organization:

Research

1. The Research and Innovation Policy Stakeholders' Arena

Please consult the accompanied research and innovation policy stakeholders' arena diagram. The diagram consists of several private and public organizations that I have encountered during my research that have a (possible) influence on the development of the RFID technology (product-level item tagging) and the METRO Group Future Store Initiative. These organizations are stratified in the local, regional, national and international level in relation to the METRO Group Future Store Initiative that is placed at the centre. The questions below are about the composition of this diagram in terms of the organizations, their interactions and their influences on each other in relation to the METRO Group Future Store Initiative (MGFSI).¹⁴⁵

Your Organization in relation to the MGFSI

- From your organization's standpoint, could you correct any organizations that are misplaced in the diagram?
- Could you state the interest of your organization in the MGFSI or other (Research and Development) activities being undertaken by the METRO Group?
- Could you state the influence/role of your organization on/in the MGFSI or other (Research and Development) activities being undertaken by the METRO Group?

Partner Organizations in relation to the MGFSI

- Could you draw 'green' lines between your organization and the organizations with which your organization has a (constructive) collaborating relation, i.e. the partner organizations (in case they are not placed on the sheet, feel free to add them)?
- Could you describe what the most important (innovation) agenda items/topics/themes/problems/issues/concerns/objectives/challenges etc. are on which your organization is collaborating with its partner organizations?
- Could you describe how the interactions, (innovation) agenda setting, negotiations and decision-making between your organization and the partner organizations take place?
- Could you describe how the strategy and/or course of action of your organization has been influenced or has been changed by these interactions and negotiations (concerning the items of the (innovation) agenda) with its partner organizations? [In other words, has your organization learned and what has it learned?]

Competing Organizations in relation to the MGFSI

- Could you draw 'black' lines between your organization and the organizations with which your organization has a competing relation, i.e. the competitors (in case they are not placed on the sheet, feel free to add them)?
- Could you describe what the most important competing elements (e.g. (innovation)

¹⁴⁵ The METRO Group Future Store Initiative (MGFSI) encompasses the activities being deployed at the REAL Future Store in Toennisvorst (RFID applied on individual meat packaging), the Galeria Kaufhof in Essen (RFID applied on individual Gardeur menswear) and the RFID Innovation Centre (RFID information an exhibition centre). The whole Future Store Initiative is supported by the METRO Group and the METRO Group Information Technology (MGI) in particular.

agenda items, products, processes, services, technologies, standards, market share, customer satisfaction, other) are on which your organization is competing with its competitors?

- Could you describe how the interactions and negotiations concerning the competing elements between your organization and the competing organizations take place?
- Could you describe how the strategy and/or course of action of your organization has been influenced or has been changed by these interactions and negotiations (concerning the competing elements) with its competing organizations? [In other words, has your organization learned and what has it learned?

Counter (balancing) Organizations in relation to the MGFSI

- Could you draw 'red' lines between your organization and the organizations with whom your organization has a 'counter balancing'¹⁴⁶ relation (in case they are not placed on the sheet, feel free to add organizations)?
- Could you describe what the most important (innovation) agenda items/topics/themes/problems/issues/concerns/objectives/challenges etc. are on which your organizations is disputing/disagreeing with the counter balancing organizations?
- Could you describe how the interactions and negotiations (concerning the (innovation) agenda) between your organization and the counter balancing organizations take place?
- Could you describe how the strategy and/or course of action of your organization has been influenced or has been changed by these interactions and negotiations (concerning items of the (innovation) agenda) with its counter balancing organizations? [In other words, has your organization learned and what has it learned?]

Relations between the other organizations

- The previous 15 questions were about your organization and its relations to other organizations either being collaborating, competing or counter balancing. Could you now indicate using the same distinctions collaborating (green), competing (black) and counter balancing (red) for the relations you know other organizations have to each other (in case they are not placed on the sheet, feel free to add them)?
- Could you describe from the standpoint of your organization what the interactions you just drew are about?

Policies, laws and guidelines in relation to the MGFSI

- Between the '<< >>' signs I have stated important policies, laws and guidelines that seem to be relevant for the employment and development of the RFID technology? Are these the right ones, are they placed on the right level and are there any missing?

¹⁴⁶ Counter balancing means that an organization is (strongly) opposing or disagreeing with the kind of activities that are being deployed, developed or experimented with at your organization. In addition, they voice their discontentment either directly to your organization and/or indirectly via other channels of communication.

- Could you describe in what way your organization is involved in constructing or contributes to shaping these policies, laws and guidelines?

Other

- Is there anything you feel like mentioning in relation to the previous questions and or the research and innovation policy arena as such?

2. Expectations, visions and influences concerning the RFID technology

Expectations about the near future (short/intermediate-term) concerning the RFID technology employment and development at the FSI / METRO Group / retail sector

- What is the near future expectation of your organization regarding the further roll out of the RFID technology applied on consumer products (product-level item tagging) at the MGFSI / METRO Group / retail sector?
- What does your organization consider to be the main issues that need to be resolved in order for the RFID technology applied on consumer products (product-level item tagging) to be further rolled out at the MGFSI / METRO Group / retail sector?

Future (long-term) visions of the RFID technology applied on individual consumer products

- What is the vision of your organization regarding the in-store application of the RFID technology on consumer products (product-level item tagging) for the FSI / METRO Group / retail sector?

External influences from the global (business) context upon the RFID employment and development

- What does your organization consider to be the most important external *stimulating* influences/factors from the global (business) context (incl. the research and innovation policy arena) upon the FSI, the METRO Group and the retail sector that play a key role in the development and employment of the RFID technology as applied on consumer products (product-level item tagging) in the in-store domain?
- What does your organization consider to be the most important external *restraining* or *hindering* influences/factors from the global (business) context (incl. the research and innovation policy arena) upon the FSI, the METRO group and the retail sector, that play a key role in de development and employment of the RFID technology as applied on consumer products (product-level item tagging) in the in-store domain?

Concluding

1. Are there interesting things that you deem relevant that need to be mentioned and or discussed in addition before wrapping up?
2. Does your organization have any key brochures / documents / flyers / folders / DVDs / / presentations / other promotion material that contains information / facts / figures (preferably in English) that may benefit my research?

Thank you for your cooperation!

