Modality Mix of RFID Regulation*

Daniel Ronzani *)
CBS, Centre for Applied ICT, Howitzvej 60, 2000 Frederiksberg, Denmark
dr.inf@cbs.dk

IBM Research GmbH, Säumerstrasse 4, 8803 Rüschlikon, Switzerland
dan@zurich.ibm.com

Abstract. This paper provides a general reflection on how law must manage the evolution of technology. By the example of radio frequency identification (RFID), it analyses the necessity of RFID regulation based on Lessig's four modalities law, norms, market and architecture. This paper suggests that a trade-off between or complementing of the four modalities is necessary for a holistic regulation of RFID. To support this claim, various topics of the draft recommendation on the implementation of privacy, data protection and information security principles in RFID applications by the European Commission of February 2008 are cross-examined with and attributed to one of the four modalities. This paper concludes that the draft recommendation does not provide precise supplementing legislation to justify its implementation. Many law-related issues of the draft recommendation can be traded off against or complemented by the other three modalities norms, market and architecture.

1. Introduction

The Internet of Things is a network of communicating devices that can interact in the context of the physical world (Buckley, 2006). In this realm, radio frequency identification (RFID) is one step "towards ubiquitous computing which together with technology-convergence may lead to seamless integration of the physical world with cyberspace" (Van de Voort, Maarten & Ligtvoet, 2006). Because (i) RFID is one of the interfaces to cyberspace and (ii) the European Commission's Directorate General Research Centre suggested that a closer look at existing legal framework for RFID along with the development of processes for establishing guidelines and best practices is needed (Van Lieshout & et al., 2007), it is justified to recall Judge Frank Easterbrook's speech titled "*Cyberspace and the Law of the Horse*" (Easterbrook, 1996). In his speech, Easterbrook argues that the best way to learn the applicable law to specialized endeavours is to study general rules. He strongly criticizes the implementation of a specialized law for new technologies:

> "We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross-sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds. […] Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers." (Easterbrook, 1996)

One of Easterbrook's arguments is that if legislators are too far behind in matching law to well-understood technology such as photocopiers (copyright), then what chance will one have for fast-living computer technology? In his opinion, it makes no sense to match an imperfect legal system to an evolving world that is understood poorly. His advice is – in a nutshell – to stick to existing laws (Easterbrook, 1996).

Lessig (1999) disagrees with Easterbrook and argues that interdisciplinary thinking is important. He offers techniques for escaping the limits of a regulator by "recognizing the collection of tools that a society has at hand for affecting constraints upon behaviour" (Lessig, 1999). According to Lessig, the tools are: law, norms, market and architecture. Many authors suggest regulating RFID with a multi-spectral approach that includes, for instance, changes in law, furthering of guidance and self-regulation, implementation of technical measures or improvement of education (Van de Voort, Maarten & Ligtvoet, 2006; Hustinx, 2007; Hübner-Fischer, 2000). However, to date there seems to be little effort to move away from enacting new laws towards embracing the other three regulatory tools envisioned by Lessig. Hence, the claim in this paper is that the regulation already enacted in Europe suffices

---

* This article was first published in Kierkegaard, Sylvia, (2008) Synergies and Conflicts in Cyberlaw, IAITL,pp. 108- 122.

*) This paper reflects the author's personal opinion.

and that the focus needs to shift towards norms, market and architecture. There is no need for additional legal regulations, such as the draft recommendation on the implementation of privacy, data protection and information security principles in applications supported by RFID in February 2008 (hereinafter "Draft Recommendation").

The debate on the applicability of Lessig's four tools concerns many new fields, in which a new technology is prevalent. The dispute is not RFID technology specific. However, RFID is a good proxy to discuss this debate since it is very topical. This discussion is organized as follows: Section 2 structures the problem as to why a mix of modalities is necessary. Section 3 offers an overview of the four modalities. In section 4, the key topics of the Draft Recommendation are first analysed and then supplemented with tentative solutions. Section 5 concludes that the Draft Recommendation by the European Commission should not be implemented because it is redundant with enacted legislation. Instead, a trade-off in favour of the modalities is proposed.

2. Problem Statement

In 2006 the European Commission conducted several workshops and a public consultation process on RFID (ICS, 2007). The European Commission noted that although most stakeholders are still unaware still being unaware of the potential and risk of RFID, opposing camps had already formed. The scope of the 2006 consultation process was to advance the debate on RFID objectively and to provide a balanced overview of the necessary action on RFID issues (Van de Voort, Maarten & Ligtvoet, 2006). In general, the survey showed that two-thirds of the 2190 respondents of the 2006 RFID consultation feel that the current legislation is inadequate and that existing laws should be modified in order to strengthen the protection of personal data and privacy. Specifically on security and privacy issues, more than half of the respondents report that some kind of legislation regulating RFID should be considered (___, 2006; COM (2007)96).

Lessig states that law alone can neither enable nor guarantee legal values. He therefore proposes four modalities of regulation (Lessig, 1999): law, norms, markets and architecture. He notes that these modalities regulate together and that, depending on the context to be regulated, there is a *trade-off* between them. Thereby a modality can influence either an individual directly or another modality that subsequently influences the individual. The goal is to find the optimal mix which depends on the plasticity of these four different modalities (Lessig, 1999).

The problem is not that Lessig's modality mix is not used today. As Table 1 shows Lessig's concept is used, albeit with different terminology. The problem is that from a holistic perspective, we risk over-regulating with law if we do not consider the trade-off between the four modalities. As noted earlier, the claim in this paper is that if norms, market and architecture are considered, this will result in less need for laws. This trade-off is possible and affordable because the technology-independent legislation enacted at European level is already sufficient to protect the stakeholders (with some limitations).

	Lessig (1999)	Hübner-Fischer (2000)	Reding (2006)
Terminology of modalities	Law	Law	European rules
	Norm	Fair information practices (FIP)	Self-regulation
	Market		Industry
	Architecture	Privacy enhancing technology (PET)	Privacy enhancing technology (PET)

Table 1: Different terminology for the same modalities of RFID regulation.

Following the first public consultation on RFID held in 2006, the European Commission issued the Draft Recommendation. In this paper the Draft Recommendation will be analysed based on Lessig's modality mix. The next section outlines the four modalities in more detail.

3. Modalities

The four modalities- law, norms, market and architecture- of Lessig's concept of behavioural constraints regulate together and the net regulation of any policy is the sum of the regulatory effects of the four modalities (Lessig, 1999). It is important to distinguish between the four modalities.

Law typically regulates behaviour by statutes. Law is regulated, controlled and enforced by government authorities. Mostly there will be a constitutional mandate to enact statutes. The statutes can envision further delegation to ordinances or regulations. The European Commission, for example, has enacted directives that need to be implemented into national law of EU member states. The protection of personal data, for instance, is covered by the technology-independent Directive 95/46/EC regardless of the means of procedures used for data processing (COM(2007)96). But there are also less enforceable regulations, such as the Draft Recommendation.

Norms regulate similarly as, but not equal to law (Lessig, 1999). Norms are non-legal rules that certain individuals feel compelled to follow despite the lack of formal legal sanctions; or stated positively, they are non-legal rules that certain individuals follow because they benefit from doing so (Carlson, 2001). Both modalities, law and norms, threaten punishment ex post. But whereas the regulation of law is centralised at authority level, the regulation by norms is decentralised by and to a community (Lessig, 1999). The sanction to be imposed by the community can be extended to third parties. Thereby, codes of conduct are created by imposing requirements on an entire community rather than merely on the interested (private) parties (Bendor & Swistak, 2001). EPCglobal, the leading standardization body for the development of industry-driven standards for the electronic product code to support the use of RFID, for instance, has issued guidelines on RFID. These are regulations that are followed and sanctioned as norms by the members of EPCglobal.

Market regulates behaviour by different influences, such as demand and supply that is reflected in price. Prices can constrain access. Lower RFID tag costs and improved RFID tag performance have opened new markets and applications for RFID (Van de Voort, Maarten & Ligtvoet, 2006). Industrial entities, for instance, are bringing RFID to market and many small- and medium-sized entities have successfully deployed RFID (COM(2007)96). However, mass implementation is price-driven and it is generally assumed that a cost reduction of passive RFID tags to less than 1 cent is necessary for a large scale adoption (COM(2007)96).

Architecture – understood by Lessig as the physical world as we find it – also regulates in the form of shaping one's behaviour. In this paper, it is argued that RFID architecture is divided into physics and systems (artefacts). On the one hand, RFID architecture has specific characteristics imposed by the physics of radio waves that direct and limit the way RFID technology can be implemented and used. For instance, the characteristic that water absorbs, metal reflects and other materials have varying effects on radio waves of passive tags (Sood, 2007). On the other hand, RFID architecture includes the structure of IT systems, like a multi-tier RFID system comprising the RFID reader, middleware and the back-end enterprise system (Lahiri, 2006).

Each section and topic of the Draft Recommendation can be attributed to one or more of the four modalities. In the following section, an analysis and a tentative solution are proposed for each of the most important sections and topics of the Draft Recommendation.

4. Discussion

Only 15% of the respondents of the 2006 public consultation viewed self-regulatory efforts by themselves adequate to regulate RFID (Reding, 2006). By cross-examining all four modalities with the topics of the Draft Recommendation, this paper shows that there is a misbalance in the modality mix of RFID regulation. Whereas it could be argued that the Draft Recommendation itself falls entirely within the modality of law (see section 3) and therefore cannot be accounted for by the other three modalities, the *topics* of the Draft Recommendation touch upon all four modalities. The analysis of these topics in the Draft Recommendation is justified in order to propose which legal modalities are best traded off against the other three modalities, i.e. norms, market and architecture.

4.1 Article 1: Scope

4.1.1 Analysis

Article 1 of the Draft Recommendation covers the scope. The Draft Recommendation provides guidance on privacy, data protection and information security to EU member states and stakeholders in a lawful, ethically admissible, as well as socially and politically acceptable way on the design and operation of RFID applications.

The scope of the Draft Recommendation is to provide guidance and therefore by nature is not compulsory. The question arises whether a guidance of this sort will provide the necessary legal certainty for the sale, implementation and deployment of RFID. As has been noted at the 2006 RFID Public Consultation Workshop on Applications and Emerging Trends, adhering to guidelines is voluntary and lacks enforcement options to protect the public from non-compliant companies. Therefore, guidelines are likely to prove inadequate to regulate privacy issues (Van de Voort, Maarten & Ligtvoet, 2006). The same will apply to security issues.

Although this Draft Recommendation aims at achieving a coherent internal market approach towards information security (article 6(2)), EU member states generally remain free to implement national legislation with or without adapting this Draft Recommendation. The scope of the Draft Recommendation has been criticised for not supporting the achievement of a coherent internal market, which is one of its main objectives. The Draft Recommendation lacks an economic evaluation for it covers legal, ethical, societal and political values, but not economic ones.

4.1.2 Tentative Solution

The proposal in this paper is twofold. First, the Draft Recommendation, or the recommendation itself cannot be viewed as a norm, regardless of which of the three theories about norm creation one follows , *i.e.,* norm internalization by Robert Cooter, esteem worthiness by Richard McAdams, or equal behaviour by Eric Posner (in: Carlson (2001)). The Draft Recommendation is issued by the European Commission as the central authority and will remain a legal, but unenforceable tool because the EU member states do not need to implement it. In contrast, the ethically admissible as well as socially and politically acceptable ways of use of RFID technology are norms. Violations of such norms can be sanctioned outside of the Draft Recommendation. To the extent that the Draft Recommendation by the European Commission remains unenforceable, it should not be implemented.

Second, if the Draft Recommendation was to be implemented nonetheless, then its scope would need to be extended to include the economic value of RFID. In order to find solutions that are acceptable to both consumers and the RFID industry, the economic aspects of RFID implementation and deployment are important. This means that the economic value will need to be addressed in the scope as well. This would extend the modalities to include the market. Regardless of whether RFID still is in its infancy with most applications not being large-scale, and the forecast for economic benefits remaining yet unclear (Van Lieshout & et al., 2007) or whether RFID is about to become very widely used (Reding, 2006), it is important for Europe to clear away legal issues that may act as barriers to a rapid deployment in RFID and to implement initiatives that will allow European citizens to benefit from RFID technology. Europe is a leading region in research and development for RFID, and Europe's economy needs to remain strong and competitive (Reding, 2006).

4.2 Article 2: Definitions

4.2.1 Analysis

Article 2 covers the definitions used in the Draft Recommendation. The definitions of "RFID application", "RFID application operator", "RFID tag", "reader" and "deactivation" are of interest because they are unclear.

The definitions of "RFID application" and "RFID application operator" are imprecise. The former seems to include an entire IT environment irrespective of its relation to RFID technology. The latter is also too broadly defined by stating "[…] person who *develops*, *implements*, *uses* or *maintains* a[n] RFID application" (emphasis added). This definition seems to include suppliers of RFID technology and services. But the Draft Recommendation also makes a distinction in article 3(3) between the "RFID application operators and *providers* of such [RFID] applications" *(emphasis added)* that is not reflected in the aforementioned definition of "RFID application operator". Hence, the definition of "RFID application operator" remains unclear as to whether the person developing, implementing, using, or maintaining an RFID application is intended to exclude the provider, or not. There are entities in the RFID market that offer a broad range of ICT services. Do these companies also fall within the definition of "RFID application operator"? Does the definition of "RFID application operator" extend to them as outsourcers if they offer outsourcing services that cover RFID technology?

Second, article 2(b) of the Draft Recommendation defines RFID tags as being an RFID device either capable of re-coupling, back-scattering or reflecting, and modulating a carrier signal received from an RFID reader; or capable of producing a radio signal. The latter function refers to active RFID tags that use the (internal) energy source not only to power the chip, but also to emit a signal independent of the influence from an RFID reader. An apparatus with such characteristics is a short-range device according to Finkenzeller (2006), Kern (2006) and Bensky (2004). This transmitter-receiver function contradicts the definition of "reader" in article 2(c) of the Draft Recommendation, which "stimulate[s] and effect[s] a modulated data response from a tag or a group of tags". Clarification on passive, semi-active battery-assisted and active tags is necessary. As has been suggested at the Internet of Things 2008 Conference (IOT 2008), legal implications could be different, depending on whether active tags are understood in a narrow or wider sense (Ronzani, 2008).

Third, the definition of "deactivation" suggests that any functionality of a tag be terminated. Regardless of the definition in the Draft Recommendation, the term "de*activation*" *(emphasis added*) suggests that in the case of a passive tag, the functionalities are active. However, this is not the case for passive tags due to their architecture. Passive tags need to be activated by a carrier signal received from an RFID reader to generate the necessary energy to re-couple, backscatter or reflect.

4.2.2 Tentative Solution

Definitions that are unenforceable and imprecise are likely to create more confusion than generate a coherent understanding. It is only when they are defined in an enforceable law would such terms add value. But since (i) the Draft Recommendation is non-binding and thus unenforceable, and (ii) technology is evolving rapidly, the laws should be technology-independent. A specific legal definition of these terms is therefore unfavourable.

Following Lessig's modality mix, it is more favourable to regulate in this situation by market and architecture. The RFID application needs to be addressed by architecture. It will provide the boundaries of what is technically possible and what is not possible. The question of who is the RFID application operator can be determined by the market.

In the light of the Draft Recommendation's focus on privacy, data protection and information security aspects of RFID technology deployment, the cessation of all functionality is unreasonable and exaggerated. A cessation of the entire functionality of a tag could ultimately lead to a cessation of deployment of RFID technology by the industry. If a deactivation is necessary at all, then it should be limited to certain functionalities only.

4.3 Article 3: Privacy Measures

4.3.1 Analysis

Article 3 of the Draft Recommendation stipulates the privacy and data protection measures to be taken by the RFID application operator. In the following paragraphs, the privacy impact assessment, the burden of proof, and its publication are discussed in more detail.

First, RFID application operators need to conduct a privacy impact assessment *prior* to the implementation of RFID applications. The Draft Recommendation foresees that its level of detail depends on the risk associated with the application. Here it is argued that the risk will eventually only be known *after* the assessment has been performed and that therefore the level of detail cannot be adjusted in a timely manner. The risk lies completely with the RFID application operator. In order not to run retrospectively the risk of not having assessed the threat correctly and thus not having applied a level of detail proportionate to such risk, an RFID application operator would always need to conduct a full-scope privacy impact assessment.

Second, the RFID application operator and the component provider need to take the "appropriate technical and organisational measures to mitigate" the risk "where it cannot be *excluded* that processed data is related to an identifiable natural person" (emphasis added). This exclusion requires negative proof evidence that is almost impossible to produce. It is likely that RFID opponents could frequently argue that processed data can be linked to an identifiable natural person somewhere in the end-to-end dataflow and that such risk could indeed never be excluded. This would render the paragraph useless.

Third, there is an option for the RFID application operator's privacy impact assessment to be made public. Such publication could probably be interpreted under certain national legislations as being a representation and warranty by the issuing entity. To this extent, it might exceed the mandatory requirements for representation and warranty of national law. Furthermore, it is not clear why the provider of components would be excluded from such publication as stipulated in article 3(3).

4.3.2 Tentative Solution

As Van de Voort, Maarten & Ligtvoet (2006) have noted, guidelines are likely to prove inadequate to regulate privacy issues. Hence, norms will not largely be a suitable modality. The risk assessment would therefore need to remain regulated by law. However, following the argument in the preceding sub-section that the risk assessment timeline is unmanageable, it is suggested that the risk assessment be omitted altogether as regulatory tool.

Burden of proof is regulated in and as a tool of process or procedural law. What proof evidence is necessary and which party needs to provide such evidence or counter-evidence are subject to national procedural legislation of the individual EU member states. It is suggested in this paper that the burden of proof remain a legal modality of national law. It is not favourable to interfere with such legislation in an unenforceable draft recommendation.

Notwithstanding the foregoing, publication of privacy measures can be regulated by guidelines, *i.e.* by norms. It seems reasonable that a (RFID) community agrees on how, and what kind of information of implemented, privacy measures should be published.

4.4 Article 4: Codes of Conduct

4.4.1 Analysis

Article 4 of the Draft Recommendation encourages trade or professional associations or organisations involved in the RFID value chain to draw up specific codes of conduct on RFID.

Article 27 of Directive 95/46/EC already stipulates an encouragement for the EU member states to make provisions for trade associations and other bodies. Article 4 of the Draft Recommendation is a partial copy of article 27 of Directive 95/46/EC, which encourages the drawing up of codes of conduct, and thus superfluous. Codes of conduct on RFID partly are already in place, e.g. the public policy guidelines by EPCglobal.

4.4.2 Tentative Solution

It has been suggested by participants of the 2006 RFID consultation workshop that a compromise between strict regulations and voluntary (and typically unenforceable) guidelines might be a possible solution. Companies would agree to high fines if they breached privacy guidelines they have accepted (Van de Voort, Maarten & Ligtvoet, 2006). According to Homans (Gibbs, 1965), a "statement made by a number of members of a group, not necessarily by all of them, that the members ought to behave in a certain way in certain circumstances" qualifies as a norm. According to Carlson (2001), codes of conduct are created by norms that impose requirements on an entire community and not merely on the interested parties. The obligation to impose a sanction can be extended to third parties, *i.e.* people unaffected by the deviation but in the position of sanctioning the deviant.

The recommendation by the European Commission to extend the legal regulations by including norms is favourable. This expansion is in line with Lessig's modality mix. To this extent, the proposal in this paper is to acknowledge that the legal provisions suffice to establish the necessary codes of conduct. The enacted provisions must not be replicated in the unenforceable Draft Recommendation. The focus needs to be on the actual establishment and strengthening of the acceptable codes of conduct by (RFID) communities.

4.5 Article 5: Information on RFID Use

4.5.1 Analysis

Article 5 of the Draft Recommendation regulates the use information of RFID. Where RFID applications are implemented in public places, a written comprehensible policy needs to be made available by the RFID application operator, such as the identity of the RFID application operator or the purpose of RFID application.

The value of this provision is limited insofar as Directive 95/46/EC already lists an extensive catalogue of information that needs to be provided by the data controller or its representative. This catalogue in article 10 of Directive 95/46/EC is a minimum requirement that includes identity of controller or representative, purpose of processing, and further information. National law can foresee more extensive regulation. In contrast to the Draft Recommendation, national legislation of EU member states is required to implement the provisions of Directive 95/46/EC into national law. Thus, the provision for information in cases of collection of data from a data subject is already set at a more stringent legislative and not only a recommendatory - level.

4.5.2 Tentative Solution

A legal solution to establish norms is favourable. This shift of regulation by law to regulation by norms is in line with Lessig's modality mix. Similar to the tentative solution in the preceding section, the proposal is to acknowledge that the current legal provisions are sufficient to establish the necessary codes of conduct and does not replicate the provision in the Draft Recommendation.

4.6 Article 6: Information Security Risk Management

4.6.1 Analysis

Article 6 of the Draft Recommendation stipulates the necessity of a state of the art security management and application-specific guidelines with best available techniques to achieve a coherent internal (i.e. European) market approach.

First, the value of this provision is unclear since the security of processing is already regulated in detail in Directive 95/46/EC. Article 17 provides that the "controller must implement appropriate technical and organizational measures to protect personal data against various processes and incidents, including unauthorized disclosure or access." Since national legislation is already required to implement Art.17 of Directive 95/46/EC, the provision in Article 6 of the Draft Recommendation becomes obsolete.

Second, the development of RFID application-specific guidelines and dissemination of best available techniques for such applications that might be exposed to information security threats should be encouraged at a European level to achieve a coherent internal market. Whereas the exchange of best practices generally seems to be a favourable approach, it is argued here that as long as the 27 EU member states are not required to implement the Draft Recommendation its impact for a coherent internal market remains questionable.

4.6.2 Tentative Solution

The three proposals in the Draft Recommendation can be evenly distributed among the three modalities- norms, market, and architecture,- because Directive 95/46/EC already sets the necessary legal boundary. As outlined in the preceding sections of this paper, a replication of the enacted legislation in the Draft Recommendation is not

necessary. It is preferable to focus efforts on the accomplishment of state-of-the-art information security management, application-specific guidelines, and a coherent internal market approach other than by legal regulations.

Issues of linking data to individual users are not RFID specific. They need to be tackled irrespective of a specific technology. With regard to RFID, they need to be addressed by 'privacy by design' and need to encompass the processes of data collection, data storage and data management (Van de Voort, Maarten & Ligtvoet, 2006). The information security management therefore needs to be attributed to the architecture modality. The Article 29 Data Protection Working Party noted that "for many applications, the tag contains only an Id whose [sic] semantics can only be accessed through a complete IT application environment. [… O]nly a small number of RFID tags bear semantic information" (Schaar, 2005). The information is likely to be stored in a back-end system. Such a back-end enterprise system would typically encompass the complete suite of applications and IT systems of an enterprise (Lahiri, 2006), i.e. application servers and databases. A database management system is software designed to manage the handling of data. It provides independent representation and storage of data from application programs (Ramakrishnan & Gehrke, 2000). It is therefore argued that the security management should take place within this architecture. This would meet 70% of the expectations of the respondents to the online consultation launched by the European Commission in summer 2006 that plead for privacy enhancing technologies to safeguard privacy (COM(2007)96).

The application-specific guidelines need to be reflected as norms. The RFID application providers and operators will need to set the guidelines. These guidelines to evolve from within the RFID provider and operator community and cannot be forced upon them from the outside, i.e. through the Draft Recommendation.

4.7 Article 7: RFID Use in Retail Applications

4.7.1 Analysis

Article 7 of the Draft Recommendation is a special clause for retailers. It proposes indication of RFID technology by requiring a sign. It includes the necessity of a legitimate after-sale purpose, and it foresees an opt-in for consumers at point of sale as well as an opt-out clause. Moreover, deactivation of the tag may not be linked to legal disadvantages.

First, retailers should adopt a harmonised sign to indicate the presence of RFID tags. This seems to be a reasonable proposition that will support the acceptance by the general public. Whether such a sign would need to be on every item, or a centralized notification by the retailer, has yet to be seen. But considering that a product can be sold after the initial purchase, it will probably be favourable to include a sign on the product itself (where possible) or on the packaging that could also be thrown away.

Second, consumers should be informed about a legitimate after-sale purpose. Article 7 of Directive 95/46/EC already stipulates the cases of legitimacy. Three of the six examples enumerated (lit. a, b and f) could apply in RFID retail: (lit. a) the data subject has unambiguously given his or her consent; or (lit. b) processing is necessary for the performance of a contract to which the data subject is party; or (lit. f) processing is necessary for the purposes of the legitimate interests pursued by the controller (except where fundamental rights are violated). Furthermore, the Draft Recommendation text and the introductory remarks to section 3(a) suggest that the only way of making data processing legitimate is by deactivating the RFID tag at point of sale unless the consumer chooses to keep the tag operational (opt-in). This interpretation of Directive 95/46/EC is challenged. According to article 14 of Directive 95/46/EC, the data subject has the right to object at any time to the data processing, especially if data is processed for the purposes of direct marketing. Hence, an opt-out possibility cannot a priori be excluded.

Third, the opt-in clause means that the retailer must by default deactivate the RFID tag at point of sale "where a[n] RFID application processes personal data, or the privacy impact assessment […] shows significant likelihood of personal data being generated from the use of the application" (Commission of the European Communities, 2008, Art. 7 para. 3(a)) unless the consumer explicitly requests the tagged item to remain "activated" (but see argument in section 4.2.1). As noted above in section 4.2, the definition of "RFID application" is very broad. It includes all IT systems attached to an RFID system. The opt-in clause stipulates the deactivation by default for all tagged retail items, even if the processing and generation of personal data occur through a back-end database and are managed by a database management system (Van de Voort, Maarten & Ligtvoet, 2006). However, it is claimed here that at retail level, RFID is a mere input technology. This means that a large part of the issues with data protection and privacy occur at application level, in particular in back-end databases (European Commission, 2006). [1]

[1] It can be referred to section 4.6.2 where the information security risk management for database management systems has been discussed.

4.7.2 Tentative Solution

A technology-specific privacy concern that has been identified with RFID is that people may be unaware that they are carrying an RFID tag, which can be read from a distance. Distant reading would apparently enable individualised identification and revealing of personal data (Van de Voort, Maarten & Ligtvoet, 2006).

First, the obligation of placing a sign on a product or on the packaging could remain a law modality if this obligation was formulated in a technology-independent way. If the obligation is RFID-specific, then a regulation by norm is more favourable. A guideline within the (RFID) community could regulate such obligation. It is suggested that if a retailer failed to adhere to a guideline it has previously adopted then the consumers would quickly sanction such misconduct by either boycotting the product or even the retailer itself owing to mistrust in such retailer.

Second, two-thirds of all respondents of the 2006 public consultation by the European Commission view the development of technical solutions allowing RFID tags to be disabled as a way to eliminate or greatly reduce the concerns of security and privacy of RFID applications (___, 2006). Nevertheless, it is argued here that the same modality and argument as discussed above for the placing of a sign alerting to the use of RFID technology could apply for the deactivation *requirement* (as compared to the *deactivation* itself in section 4.2): the requirement to deactivate can be regulated by a guideline, a norm. Should a retailer fail to adhere to a norm it previously accepted, then the consumers would most probably sanction such (mis-)behaviour with direct consequences for the retailer. However, it must be emphasized again that, for instance in retail, (passive) RFID tags are likely to contain only a product code. This would make a person identifiable, but only if the eavesdropper has access to the (back-end) database where the data of the customer is stored. The point here is that in retail, neither a barcoded nor an RFID-tagged item is likely to directly include personal data of the consumer (Schaar, 2005). In either case, the item will only carry a product code (UPC or EPC in this example). Thus, if the personal data is not stored directly on an RFID tag and therefore not directly accessible, a differentiation between barcoded and RFID-tagged items and a deactivation of the RFID tag at point of sale as compared to barcodes not being removed at point of sale, is unjustified even if barcodes require line of sight for the read and RFID tags do not. A deactivation or removal can be considered only when personal data is stored directly on the tag, i.e., if there are no security measures in place such as encryption.

Participants of the 2006 RFID consultation claimed that databases may not be secure enough and that criminals might illegally use data collected in such databases (Van de Voort, Maarten & Ligtvoet, 2006). Following the general principle of criminal law "nulla poena sine lege", the terms *criminal* and *illegal use* imply that a law is being breached. Why then enact yet another law if the laws already sanction illegal use? Remedies and sanctions for breach of the law are regulated at national EU member state level, for instance in Directive 96/9/EC and national criminal law.

Finally, the necessity of a legitimate after-sale service is likely to be regulated by the market. If the suppliers of goods and retailers offer additional services (free of or at charge) and the demand for such services increases, this could be a legitimate argument for promoting after-sale services.

4.8 Article 8: Awareness Raising Actions

4.8.1 Analysis

Article 8 of the Draft Recommendation addresses RFID awareness.

Although the explanation to article 8 of the Draft Recommendation suggests that both the general public and enterprises, especially SMEs, be informed about the benefits and risks of RFID technology, the text of the Draft Recommendation only mentions "companies, in particular SMEs". It is unclear why governments, administrations and especially the general public are omitted from the enumeration in the Draft Recommendation. Administrations are large user groups of RFID technologies, such as the U.S. Department of Defense, and the use of RFID technology is likely to increase in the public sector.

4.8.2 Tentative Solution

Two-thirds of all respondents of the 2006 public consultation view the development of awareness raising campaigns to educate consumers as way to eliminate or greatly reduce the concerns of security and privacy of RFID applications (___, 2006). The efforts to increase the awareness of the government and the general public need to improve greatly. It is therefore necessary that governments and administrations adhere to the same principles as the industry. Furthermore, the general public needs to be informed and educated on RFID technology, threats and risks. Consumers are mature and, with sufficient awareness-raising, quite capable of making their own informed decisions.

5. Conclusion

In the RFID space, polarizing solutions are generally not favourable. A balance must be found in many cases. For instance, if RFID were to be legislated to the last detail, the following two extreme scenarios could be envisioned:

(i) Law is (entirely) in favour of the consumer. In order to fulfil the legal requirements, the RFID industry would need to invest disproportionately to meet the requirements of the law. This would lead to an uneconomic business case and subsequently to the RFID industry reducing or even ceasing its investments in RFID. The RFID market would collapse.

(ii) Law is (entirely) in favour of the RFID industry. The RFID industry would invest in RFID, and the RFID market would initially grow. But consumers, to whose disfavour the enacted legislation would be, would counter-react by boycotting the market. Sales would shrink. The RFID market would also collapse.

Draft Recommendation by European Commission		**Modalities**			
Sections in Draft Recommendation	Selection of topics in Draft Recommendation	Law	Norms	Market	Architecture
Scope	Law	■ O			
	Ethics	■	O		
	Society and Politics	■	O		
	Economy	-		O	
Definitions	RFID application	■			O
	RFID application operator	■		O	
	Tag	■			O
	Reader	■			O
	Deactivation	■			O
Privacy Measures	Risk assessment	■ -			
	Burden of proof	■ O			
	Publication	■	O		
Code of Conduct	Specific codes of conduct	■	O		
Information on RFID Use	Public places	■	O		
Inform. Security Risk Management	State-of-the-art information security management	■			O
	Application specific guidelines	■	O		
	Coherent internal market approach	■		O	
Retail	Signs	■	O		
	Legitimate after-sale	■		O	
	Opt-in / opt-out	■	O		
	Deactivation requirement	■	O		
Awareness raising	Companies and SMEs	■	O		
	Government and general public	-	O		
	Good practices in RFID appl. implementation	■	O		

Table 2: Matrix of Draft Recommendation with Lessig's Modalities. Legend: ■ indicates where the topic is currently attributed in the Draft Recommendation; O shows where the topic might be more effectively used in the modality mix; - indicates a topic that is either not addressed or should not be addressed in the Draft Recommendation.

Whereas research on the understanding of RFID technology by legal experts has shown that the understanding of RFID technology by legal experts is indeed not always beyond doubt (Ronzani, 2008), generally arguing for multidisciplinary dilettantism is exaggerated. A differentiated approach seems justified. In the past twelve years since Easterbrook's critique on interdisciplinary law and technology, much progress has been made in these two fields. But this progress does not necessarily mean that a new law needs to be enacted for every new technology. As has been shown in this paper, general rules of technology-independent legislation suffice to regulate and protect the users and stakeholders of RFID systems.

The various legal recommendations proposed do not provide precise supplementing legislation as suggested by Easterbrook (1996). Technology-independent regulations should not be complicated and diluted by recommendations that address the same issues. There are no additional benefits in the Draft Recommendation for

RFID users and stakeholders as compared to the already existing, afore-mentioned directives. The recommendations are largely redundant with existing mandatory legislation. Issuance of yet another recommendation would be over-regulating and is not to be favoured.

Instead, as has been suggested in the discussion of this paper, the topics of the Draft Recommendation are likely to be more effective if shifted towards one of the other three modalities. Table 2 summarises the discussion of this paper. The topics of the Draft Recommendation are listed in the vertical and the modalities are listed in the horizontal. The Draft Recommendation itself is the law modality. Hence, all the square boxes (■) are in the law column. As discussed in this paper, the *topics* of the sections in the Draft Recommendation provide trade-off possibilities. Table 2 shows that an extension to the other three modalities of regulation as outlined in this paper has proven appropriate. The shift is indicated in the columns of norms, market and architecture with a circle (o).

The conclusion is that net regulation (Lessig, 1999) and trade-off are not only necessary in the RFID space, but are encouraged. It is viable to reduce the legal regulation by not implementing the Draft Recommendation. The topics of the Draft Recommendation can largely be re-distributed to the other three modalities of norms, market and architecture. Table 2 suggests that following the topics of the Draft Recommendation will take more regulation by norms than market or architecture to effectively regulate RFID. But that in any case a modality mix is necessary for RFID regulation.

References

1. ___. (2006). The RFID Revolution: Your Voice on the Challenge, Opportunities and Threats. Online Public Consultation - Preliminary Overview of the Results.
2. COM(2007)96. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Radio Frequency Identification (RFID) in Europe: Steps towards a policy framework . COM(2007)96 final.
3. Bendor, J., & Swistak, P. (2001). The Evolution of Norms. The American Journal of Sociology, 106(6), 1493.
4. Bensky, A. (Ed.). (2004). Short-range Wireless Communication (2nd edition). Amsterdam: Elsevier.
5. Buckley, J. (2006). From RFID to the Internet of Things - Pervasive Networked Systems (Conference Organised by DG Information Society and Media, Networks and Communication Technologies Directorate No. Final Report). Brussels, Belgium.
6. Carlson, A. E. (2001). Recycling Norms. California Law Review, 89(5), 1231.
7. Draft Recommendation on the Implementation of Privacy, Data Protection and Information Security Principles in Applications Supported by Radio Frequency Identification (RFID): Your Opinion Matters, (2008).
8. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, (1995).
9. EC, Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, O.J. L. 77/20U.S.C. (1996).
10. Easterbrook, F. H. (1996). Cyberspace and the Law of the Horse. The University of Chicago Legal Forum, 207.
11. European Commission (2006). Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID).
12. Finkenzeller, K. (2006). RFID Handbuch (4. Auflage ed.). München: Hanser.
13. Gibbs, J. P. (1965). Norms: The Problem of Definition and Classification. The American Journal of Sociology, 70(5), 586.
14. Hübner-Fischer, S. (2000). Privacy and Security at Risk in the Global Information Society. In B. Loade (Ed.), Cybercrime. London: Routledge.
15. Hustinx, P. (2007). Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: Steps towards a Policy Framework. COM (2007) 96. Brussels. Belgium.
16. IOT (2008). International Conference for Industry and Academia 2008. http://www.iot2008.org (last accessed on 1. June 2008).
17. ISC (2007). Information Society Consultations (17. January 2007). http://ec.europa.eu/information_society/tl/activities/consultations/index_en.htm#open_consultations (last accessed 1. June 2008).
18. Kern, C. (2006). Anwendung von RFID-systemen. Berlin: Springer.
19. Lahiri, S. (2006). RFID Sourcebook. Upper Saddle River, New Jersey: IBM Press.
20. Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. Harvard Law Review, 113, 501.
21. Ramakrishnan, R., & Gehrke, J. (2000). Database Management Systems (2nd ed.). Boston, M.A.: Mc Graw Hill.

22. Reding, V. (2006). RFID: Why we Need a European Policy. SPEECH/06/597. Brussels, Belgium.
23. Ronzani, D. (2008). Why Marketing Short Range Devices as Active Radio Frequency Identifiers Might Backfire. The Internet of Things, Zurich. LNCS 4952 214.
24. Schaar, P. (2005). Working Document on Data Protections Issues Related to RFID Technology. 10107/05/EN WP 105. Brussels, Belgium.
25. Sood, P. (2007). The Physics Behind RFID. Unpublished manuscript at http://www.rfidjournalevents.com/liveeurope2007/pdfs/Nov6_University_13-15_physicsBehindRFID.pdf (last accessed 4. June 2008 - restricted website)-
26. Van de Voort, Maarten, & Ligtvoet, A. (2006). Towards an RFID Policy for Europe. Prepared for the European Commission, Directorate General Information Society and Media. DRR-4046-EC.
27. Van Lieshout, M., & et al. (2007). RFID Technologies: Emerging Issues, Challenges and Policy Options, Executive summary. EUR 22770 EN.