RFID and Privacy

Marc Langheinrich

Institute for Pervasive Computing, ETH Zurich, 8092 Zurich, Switzerland
langhein@inf.ethz.ch

Summary. RFID technology has become one of the most hotly debated ubiquitous computing technologies, and public fears of its alleged capability for comprehensive surveillance have prompted a flurry of research trying to alleviate such concerns. The following chapter aims at introducing and briefly evaluating the range of proposed technical RFID privacy solutions. It also attempts to put the problem of RFID privacy into the larger perspective of both applications and policy, in order to properly assess the feasibility of the discussed solutions.

What is it that makes RFID technology such a controversial issue these days? Seasoned newsreaders might be reminded of the heated discussions surrounding the introduction of the printed bar code in the 1970s,[1] where the comprehensive numbering of supermarket items fueled fears of a dawning apocalypse [28]. But what used to be the domain of conspiracy theorists and christian fundamentalists has since spread to average consumers who increasingly see their privacy threatend by hidden spychips that would potentially allow retailers, governments, and crooks to secretly monitor an individual's habits, behavior, and movements.

Most obvious is the rise of general concern on the Web: Between November 2003 and March 2006, the same set of Google queries for "RFID" and "RFID and privacy" not only saw an forteenfold increase in RFID-related pages (from roughly half a million to over 80 million), but also an increasing share of those mentioning privacy concerns, rising from 42% up to 68% in November 2005.[2] Internet campaigns such as CASPIAN's 2003 "Boycott Benetton"[3] and the German 2003 Big Brother Award for the Metro group,[4]

[1] On June 26, 1974, the first product with a bar code was scanned at a check-out counter. It was a 10-pack of Wrigley's Juicy Fruit chewing gum, which is now on display at the Smithsonian Institution's National Museum of American History.

[2] Measurements by the author. The general idea, as well as the November 2003 numbers, go back to Ravi Pappu [27].

[3] See www.nocards.org and boycottbenetton.org

[4] See www.bigbrotherawards.de/en/2003/.cop/

a large retailer, repeatedly warn that RFID would "create an Orwellian world where law enforcement officials and nosy retailers could read the contents of a handbag – simply by installing RFID readers nearby" [9].

At the same time, consumer surveys seem to paint a different picture. A recent European study [6] finds that only 18% of consumers have even heard of RFID technology, and that only 8% of those view its use unfavorably. Advocates point out that RFID technology already enjoys widespread acceptance across a wide variety of applications, such as car immobilizers, contactless ski passes, automated toll gates, and RFID-based payment systems. None of these systems, it seems, so far induced consumer concern or privacy issues.

This chapter primarily attempts to disentangle the intricacies surrounding today's public debate on the widespread deployment and use of RFID systems. In doing so, it will briefly survey the currently proposed technical solutions to RFID privacy and try to assess their feasibility. However, it will also attempt to clearly state both the capabilities and the limits of the technology behind RFID, as well as evaluate the practicality of commonly cited privacy invasions from RFID, especially in light of alternative (and maybe much more effective) methods of data solicitation.

1 RFID Primer

With all the potential doomsday scenarios critics like to associate with the use of RFID systems, why would anybody even consider doing this? This is because RFID systems offer three distinct advantages over traditional identification systems:

1. *Automation:* While optical bar codes require a line-of-sight for readout, i.e., either careful orientation of tagged goods with respect to the reader, or manual intervention, RFID tags promise unsupervised readouts. This increases the level of automation possible, as tagged items do not need precise orientation during the readout process.[5]
2. *Identification:* RFID tags also offer a much higher information density (and thus ultimately capacity) than bar codes, allowing manufacturers and vendors to not only store a generic product identifier on an item (e.g., "This is a bar of lavender soap"), but an individual serial number (e.g., "This is lavender soap, bar 293813"), which in turn can point to a database entry with detailed item information (e.g., "produced on May 14, 2005, in plant 5, unit 67").
3. *Integration:* The wireless coupling between reader and tag also allows manufacturers to integrate tags unobtrusively into products, thus freeing product design as well as making identifiers more robust (e.g., protection from dirt, but also against removal).

[5] See section 1.1 in this chapter for practical limitations.

The primary use of an RFID tag is for the purpose of *automated identification*, or *AutoID* for short. This is exactly what its predecessor – the bar code – was created for: In 1948, a local food chain store owner had asked researchers at the Drexel Institute in Philadelphia for a way to automatically read the product information during checkout [5]. Similarly, RFID technology is now being hailed as the next step in checkout-automation, completely eliminating checkout-lines as shoppers can simply walk through a supermarket gate and have all their items automatically billed to their credit card within seconds.

However, another set of applications additionally requires not only identification, but also authentication. The idea of *token-based authentication* is that both items and users can be reliably identified, based on an unforgeable token that they carry.[6] Users can thus prove their entitlement for a specific service (e.g., to enter a building) while items can prove their authenticity (e.g., an expensive watch, organic food, or medical drugs). One of today's most ubiquitous RFID applications, the car immobilizer, is a good example. Here, a transponder embedded into the car key will be able to reply with a proper identification when read (i.e., when put into the ignition), thus identifying itself as the proper key.[7] A fourth reason for using RFID is therefore its support for secure authentication:

4. *Authentication:* RFID tags can provide for a much stronger authentication than bar codes, as they can prevent unauthorized duplication (either through cryptographic means or by database lookups for detecting duplicates).

Similar applications are wireless ticketing systems (e.g., ski-passes), wireless payment systems (like the ExxonMobil SpeedPass[8]), and of course the recently developed biometric Passport (ePass) standard.[9] All of these require non-trivial cryptographic support in the RFID tag, as those need to be safe from cloning and counterfeiting. Otherwise, attackers could simply make up their own tags (counterfeiting) or copy a valid original (copying) and thus gain free skiing, free gasoline, or free entry. Besides the general convenience of RFID with its automated reading, the resistance to cloning attacks is thus another big advantage over the traditional bar code. While authentication applications can in principle also be implemented using bar codes, these cannot be protected from duplication attacks, thus requiring an online verification to identify duplicated tokens.

---

[6] Other ways of authenticating people would be based on "what you know" (e.g., a password), "what you are" (i.e., biometric identification), "where you are" (i.e., your location), and "what you do" (personal traits).

[7] Note that this is separate from being able to open the car doors remotely. For this, a battery-powered infrared or radio transmitter typically sends an encrypted pulse to the car. Those two might share the same key casing, however.

[8] See `www.speedpass.com`.

[9] See `www.icao.int/mrtd/publications/doc.cfm`.

1.1 Technology Overview

RFID systems are composed of RFID tags and at least one RFID reader. RFID tags are attached to the objects to be identified, while the RFID reader reads from and possibly also writes to the tags. RFID tags consist of a so-called coupling element for communication (and potentially also for supplying the tag with energy) and a microchip that stores, among other things, data including a tag identification number. The reader forms the radio interface to the tags and typically features some internal storage and processing power in order to provide a high level interface to a host computer system to transmit the captured tag data.

While all RFID systems are made up of these two components – a reader and a number of tags – a wide variety of different RFID systems exist that address the requirements of individual application scenarios. Finkenzeller [12] provides a comprehensive classification of the various commercially available RFID systems, while Want [34] offers a succinct introduction to the general principles.

RFID tags can be categorized into two classes: *Passive* RFID tags do not possess their own power supply – the reader supplies the tags with power through the coupling unit along with data and clock pulses. *Active* RFID tags, on the other hand, feature a battery in order to extend their tranmission range and reliability.[10] Most of today's privacy concerns focus on applications utilizing passive RFID tags: smart checkouts in supermarkets through tagged merchandise; human identification through tag injections under the skin; RFID-tagged banknotes, medical drugs, or luxury goods for preventing counterfeiting; or passports with embedded tags for the secure storage of biometric data. Popular articles, however, often like to quote the capabilities of *active* tags when discussing the implications of RFID deployment, thus arriving at powerful surveillance scenarios based on the significantly higher read ranges of the battery-powered models. Obviously, both prices and battery sizes will prevent the use of active RFID tags in most consumer scenarios (e.g., on cans, chewing-gum packs, banknotes, or in passports).

Passive RFID systems typically operate in one of five frequency bands: between 100-135 kHz (LF, or low frequency), at 13.56 MHz (HF, or high frequency), at 868/915 MHz (UHF, ultra high frequency),[11] and at 2.45 and 5.8 GHz (MW, or microwave). The actual frequency band used in a particular application is relevant to the privacy discussion as the laws of physics – and in particular the propagation characteristics of electromagnetic waves – set different boundaries in each of those areas, which ultimately determine much of the capabilities of an RFID system.

[10] There are also *semi-active* tags that have an internal battery for powering their microchip, yet use the reader's energy field for actually transmitting their data, allowing them to use much smaller batteries.

[11] The 868 MHz band is only licensed in Europe, while it is at 915 MHz in the U.S.

This is mainly due to a process known as *coupling* – the process of energy transfer between two different media. As tags in passive RFID systems do not come with their own power supply, the reader must supply the tag with sufficient energy to both process its commands and transmit back the reply. It can do so wirelessly – through its radio signal – with the help of the tag's coupling element, either through *electromagnetic* or *inductive* (magnetic) coupling.[12] The reader's signal thus not only communicates commands to the tag, but also powers the tag's microprocessor and allows the tag to send back its reply.

Inductive coupling, used in both HF and LF systems, works very much like a transformer, though with much lower efficiency.[13] For this to work, the tag must be within the reader's magnetic field (called the *near field region*), as further away all of the field's energy breaks away from the antenna and becomes an electromagnetic wave commonly known as a radio signal (called the *far field region*). The range of this boundary is inversely proportional to the employed frequency [33] – in HF system, for example, it lies around 3.5 m. Since beyond this range all field waves detach themselves from their originating antenna, it impossible to use inductive coupling in the far field [12]. Consequently, inductively coupled LF and HF tags cannot be powered (and thus read) from further afar than the range of the near field. In practice, read ranges are typically much smaller, as the magnetic field strength in the near field also diminishes with the power of three over the distance between reader coil and tag, resulting in read ranges of typically less then 1.5 m for LF and around 1 m for HF systems [24]. Even though larger antenna coils in both readers and tags can mitigate this effect, physical size constraints in many applications limit antenna sizes and thus read ranges.

Systems operating in UHF and MW instead employ *electromagnetic* coupling in the *far field*, similar in principle to crystal-set radios.[14] Instead of coils and magnetic fields, electromagnetic coupling uses dipole antennas and radio signals on both readers and tags. However, the energy in far field communication follows an inverse square law for both sending energy to the tag and receiving a return signal, thus yielding a $1/d^4$ law for the overall communication channel [33].[15] Highly sensitive electronics inside UHF- and MW-readers allow them to decode the backscattered signal from the tags, typically yielding

[12] It is also possible to use *capacitive coupling*, i.e., having capacitors in both the tag and the reader. However, this only works for very small distances, and is only used to *communicate* with the tag, not to power it (energy is typically supplied using inductive coupling in such systems) [12].

[13] The reader creates an alternating current in a coil that generates an alternating magnetic field, which in turn interacts wirelessly with the tag's coil (i.e., its coupling element) to induce a corresponding current inside the tag.

[14] Crystal-set radios are able to operate without batteries as they capture enough energy from the received radio signal.

[15] Note that in contrast, inductive coupling does not need a separate return signal to communicate from reader to tag – information is transmitted by changing the amount of energy the tag draws from the field.

higher read ranges than their LF or HF counterparts (up to 5-7 m). Future tags are expected to require less energy from the reader, thus increasing the potential read range of such systems even further. However, the overall signal attenuation will still continue to limit nominal read ranges to some reasonable distance (i.e., dozens, not hundreds, of meters).

The choice of coupling technology also influences the *anti-collision* protocol employed to regulate the communication between a reader and multiple tags. Regulation is necessary as tags do not have the means to detect other tags nearby. This would result in multiple tags answering concurrently to the same reader request, thus potentially interfering with each other's modulated or backscattered replies. As the anti-collision protocol governs the lower level communication between tags and readers, which potentially includes tag IDs and thus might allow eavesdropping, its choice also influences privacy risks.

UHF and MW systems typically use a *deterministic* anti-collision protocol based on binary trees, in which the reader systematically queries each possible ID-prefix. As long as the reader detects a collision (i.e., if two or more tags with the same prefix as indicated by the reader are within range), the reader increases the length of the prefix (e.g., by adding a "1" to it) until a single tag ID can be "singularized." It then replaces the bit it added last with its inverse and continues – should more collisions occur – to increase the length of the prefix [25]. The advantage of this scheme is that the reader will eventually read every tag within range, though it requires high data rates in order to be practically feasible.

Slower LF and HF systems use *probabilistic* methods instead, based on the so-called "slotted ALOHA" algorithm: The reader first sends out the number of timeslots it is willing to wait for an answer to all tags within range. Tags then randomly pick one of these slots and send their reply only when their time has come. Setting this initial number of timeslots is difficult. If the reader picks too many slots, most timeslots will be empty and thus time gets wasted. If it decides on too few, many tags will attempt to reply at the same time, resulting in signal interference and thus requiring another query round. In such instances, readers typically instruct tags that they have already identified to remain silent in subsequent rounds, in order to speed up the identification process of the remaining tags. While probabilistic methods can operate more efficiently than deterministic ones, they cannot guarantee that all tags within range can be identified within a given time.

1.2 RFID Limitations

While the possibilities of RFID are certainly impressive, both the laws of physics and (even more so) practical concerns often limit what is possible. For example, when it comes to RFID read ranges, *higher* may not always be *better*. Many RFID applications require the identification of a *particular* item (or set of items) in a particular location, e.g., the contents of *your* grocery bag at the checkout, not the items of the person behind you in line; the

validity of *your* skipass, and not the one of the person behind you in line; the authenticity of *your* passport, and not the one behind you at border control. As such, the fact that one might be able to construct a system with much higher read ranges *in principle* does not mean that the application would work better – in most instances, this would only increase the rate of false readouts. This is especially important to keep in mind when arguing about the capabilities of future systems, as a common reply to today's technical limitations is the spectre of future progress: "While this [range limitation] may be true today, industry experts say plans for building far more sensitive RFID signal receivers are in the works" [9]. Even if one could construct a system with such an improved readout capability (again, within the physical limits), most applications might not work at all with such increased ranges.

However, as [15] points out, the envisioned (so-called *nominal*) read range of a system is actually only partly relevant. While a system might be *built* to support only a few centimeters read range, a determined attacker might still achieve larger distances (the *rogue read range*) by using larger antennas and/or higher signal transmission power. For example, [22] claims that a HF tag with a nominal read range of about 10 cm can be read from up to 50 cm, while [23] reports some 30 meters for reading a single UHF tag (nominal read range: less than 10 meters).

The *tag-to-reader eavesdropping range* can even be larger than the rogue read range, as a second reader might simply overhear the signals being sent back from a tag to a legitimate reader, without itself having to be close (or powerful) enough to actually power the tag. Last not least, the *reader-to-tag eavesdropping range* is typically much larger than any of the above ranges, as even legitimate readers must operate at power levels that not only transmit information (i.e., commands) to the tags, but also supply enough energy to the tag to process and reply these commands. Consequently, their signals can potentially be received hundreds of meters away [15].

Of course, reports on record-setting RFID read-ranges must be taken with a grain of salt. This is because read records are often achieved under idealized conditions, such as simulators or lab environments. For example, the UHF read range record as reported in [23] used two very large directional antennas with a laser viewfinder in order to optimally focus its field on a specific tag – hardly equipment that would be easy to hide, let alone predictably use on moving targets (e.g., shoppers). Finke and Kelter [11] report eavesdropping on an HF-tag interchange from as far as three meters, though their snooping antenna had to be aligned perfectly with the legitimate reader's antenna, and they concede that they would need a large number of repeated (identical) readouts to actually decode the received signal.

This is due to the nature of electromagnetic coupling, where the orientation between tags and the reader antenna does affect the potential energy transfer to the tag. Ideally, tags are orientated parallel to the reader's antenna. In the worst case, however, a tag that is oriented completely perpendicular to an antenna might not receive any energy in the process, and would thus not be

detected at all. This is why many industrial solutions actually use multiple readers with different antenna or coil orientations, e.g., placed sequentially along a conveyor belt, to pick up a tag no matter its orientation.[16]

Another problem for the practical use of RFID tags is the sensitivity of electromagnetic fields to the materials in close proximity to the tags, especially water[17] for UHF and MW tags, and ferrous metals for just about any RFID tag. The carefully tuned RF circuits of an RFID system will often only operate under the planned circumstances and will become detuned when placed next or near to a non-envisioned material, or even another tag (this effect is called *tag detuning*).

Last not least: Size does matter. While a number of manufacturers already offer sub-millimeter sized RFID tags (e.g., Hitachi's current generation mu-chip has a size of less that 0.2 mm^2, its next generation will have only about 0.02 mm^2), these numbers usually do not include the antenna size. Without any antenna, or an equally small one, the effective read range of such tags is only a few millimeters, again limited by the laws of physics. Converseley, tags with a larger read range would need larger antennas as well, making it difficult to hide them maliciously.

2 RFID Privacy Challenges

If the previous section provided one fact about RFID systems, it would be that their effective use requires careful planning and controlled deployment. While specific applications (car immobilizer, factory supply chain management, etc.) can be designed in such a way that these factors are minimized, the list of potential problems – tag detuning, orientation problems, radio interferences – will most likely render RFID systems impractical for the use as a general surveillance infrastructure. However, even when discarding the often exgaggerated capabilities of RFID tags, these still represent a significant privacy problem – at least in principle – due to their enhanced means for identification. The above mentioned advantages of RFID are in this respect its biggest drawbacks:

1. *Automation:* Reading an RFID tag does not require the help of the person carrying the tag, nor any manual intervention on behalf of the reader. Thus, simple reader gates can easily scan large numbers of tags, making data acquisition much easier.

[16] Note that due to signal interference, two or more readers cannot operate in parallel, so a more space constrained solution would require switching multiple readers and/or antennas on and off in order to achieve the same effect.

[17] Humans are an excellent source of water, with more than half of the body mass being water. Similarly, groceries like tomatoes, or of course juices and soda, seriously affect RF fields.

2. *Identification:* The ability to identify individual items instead of only whole classes of items significantly improves the ability to identify an individual. This would facilitate, e.g., the creation of detailed consumer or citizen profiles.
3. *Integration:* Not only that the act of reading a tag can be completely hidden from the tag carrier (especially when operating at larger distances), also the fact that a tag is present in a particular product will be hard to ascertain for an individual without special detection equipment.
4. *Authentication:* The above points become especially critical given the increasing amount of sensitive information, e.g., health information, payment details, or biometric data, that are stored on or linked to tags used in authentication systems.

These four attributes of RFID applications threaten two classes of individual privacy: *data privacy* and *location privacy*. The location privacy of a person is threatened if a tag ID that is associated with that person is spottet at a particular reader location. These IDs do not need to be unique – Weiss et al. [35] point out that certain combinations of non-unique tags might still form unique *constellations* of items that can be used to identify an individual. Knowing that a person's car has been detected passing a certain toll station, or that a person's shoes have entered a particular building, allows others to infer (though not prove) the location and ultimately the activity of that person.

Once tags carry more than just an identifier, but also a person's name or account number, data privacy may be violated. This happens if unauthorized readers eavesdrop on a legitimate transaction, or if rogue readers trick a tag into disclosing its personal data. A special case of data privacy are product IDs that disclose the (otherwise not visible) belongings of a person, e.g., the types and brands of clothing one is wearing, the items in one's shopping bag, or even the furniture in a house. Note that in the latter case, the actual *identity* of the victim might very well remain unknown – it might be enough to know that *this* person carries a certain item.

2.1 Consumer Fears

There are three principal ways of violating an individual's data and/or location privacy: clandestine scanning, eavesdropping, and data leakage:

- *Clandestine Scanning:* The tag data is scanned without the tag-carrier's consent. This might disclose personal information (data privacy) either indirectly, e.g., by revealing the contents of bags that one cannot see through otherwise, or directly, e.g., by revealing personal data such as the name of a user or the date that a particular item has been bought. If several clandestine scans are pooled, *clandestine tracking* can reveal a data subject's movements along a tag reading infrastructure (location privacy).
- *Eavesdropping:* Instead of reading out a tag directly, one can also eavesdrop on the reader-to-tag channel (or even the tag-to-reader channel) and

receive the IDs of the tags being read due to the employed anti-collision protocol.

- *Data Leakage:* Independent of the actual RFID technology is the threat of having applications read out more information from a tag than necessary, or storing more information than needed. This is of course a threat common to all data gathering applications, though the envisaged ubiquity of RFID-based transactions renders it highly relevant in this context. Fabian and Spiekerman [10] also point out the vulnerability of the underlying commercial product information network to data disclosure attacks.

So how would an RFID privacy violation look in practice? Andrew Kantor, a columnist for USA Today, envisions the following: "A department store's RFID system recognizes that you're carrying an item you bought there last week. Now it knows who you are. And if there are readers scattered about, it knows where you're going. Come home to a phone call, 'Mr. Kantor – we noticed you were shopping for a television. . . ' " [20]. Forbes Magazine predicts: "As the shopper enters the store, scanners identify her clothing by the tags embedded in her pants, shirt and shoes. The store knows where she bought everything she is wearing." [30] These *shopping scenarios* and the associated *profiling* are probably the most widespread RFID privacy fears.

Criminal scenarios are almost as prevalent: "Sophisticated thieves walk by homes with RFID readers to get an idea of what's inside. Slightly less sophisticated thieves do the same thing in a parking lot, scanning car trunks" [20] and "Using mobile readers, future pickpockets could find out how much cash someone would carry"[18] [37]. Potential criminal activities are not only confined to burglary: "In the future, there will be this very tiny microchip embedded in the envelope or stamp. You won't be able to shred it because it's so small. . . Someone will come along and read my garbage and know every piece of mail I received" [29].

Also high on the list are comprehensive *surveillance scenarios*, where critics foresee "the development of a seamless network of millions of RFID receivers strategically placed around the globe in airports, seaports, highways, distribution centers, warehouses, retail stores, and consumer's homes, all of which are constantly reading, processing, and evaluating consumer behaviors and purchases" [9]. This seems especially likely with the use of RFID tags in passports: "Would you mind if your passport would hide an RFID chip with all kinds of private data in it? Government agencies and corporations could find out where you are, what car you drive at the moment, which ailments you have, or if you receive unemployment benefits"[19] [37]. This fear is also kindled by recent reports of RFID implants for both leisure [7] and work [31].

Interviewing 30 consumers about their concerns with respect to RFID, Berthold et al. [4] additionally identified the fear of being held responsible for RFID-tagged objects (e.g., by tracking down perpetrators of minor offenses

[18] Translation from the German original by the author.
[19] Translation from the German original by the author.

such as soft-drink bottles being discarded in public parks), and fears pertaining to the use of RFID to control the behavior of consumers (e.g., smart fridges that limit the number of soft drinks being dispensed).

2.2 Privacy Threats

Obviously, some of the above scenarios are more likely than others. It is surprising, however, that the most prominent examples are also often the least plausible ones.

Take for example the threat of covert profile building by scrulpous marketers and retailers, banding together to observe your every moves and then surprising you with deep insights into your current (commercial) needs and wishes. Not only would such behavior be illegal in most countries that feature data protection laws, retailers would also risk alienating potential customers with such overt spying, should this fact ever be disclosed. But why spy on your customers if they would give you the information voluntarily? The example of consumer loyalty cards show that many consumers are willing to have their personal data recorded in commercial databases – in return for tangible benefits (e.g., miniscule discounts). The real threat to shopper's privacy would thus lie much more with their own desire to peruse future RFID-based loyalty programs, than in sinister plots to secretly monitor them against their will.

Criminal scenarios seem equally implausible. A thief looking for wealthy shoppers might simply wait in front of a high street jewlery shop, or look out for shoppers carrying huge oversized boxes out of electronics stores with the words "plasma TV" written across. The discussion on tag detuning in section 1.2 above should have made clear that scanning a car's trunk would be as impossible as scanning the content's of a house (the latter example would also fail based on reading range alone, unless thieves would resort to parking a car with a huge antenna dish mounted on top – hardly unobtrusive). Again, the real threat lies much more with the proliferation of insufficiently secured token-based access control systems, such as electronic payment cards or biometric passports. Several researchers have demonstrated that the security of these systems can often be easily broken, resulting in more or less severe forms of identity theft [16, 26].

Having governments use RFID to build a comprehensive surveillance infrastructure is probably the least likely development. Industry groups estimate costs of well over a trillion dollars to create a "national spy network" in the U.S., covering all airports, rail and bus terminals, public offices, libraries, schools, parks, stores, etc. [1]. Additionally, given the trivial means of disabling for example the RFID tag in a passport through shielding, such an infrastructure would hardly be difficult to circumvent. Implants could equally be shielded with a corresponding metallic mesh fabric, though the small size of implantable chips as well as human tissue anyway typically imply a maximum reading distance of a few centimeters only – hardly suitable for readout without the subject's consent. Instead, the increased amount of RFID-based data

traces might, similarly to today's mobile phone and ISP connection records, create a desire by law enforcement to access logs of commercial providers in case of a particular crime or threat. As such, the fears reported by Berthold et al. [4] of an increase of direct control through traceable items strike much closer to home.

This is, then, the true danger of RFID technology to our privacy: its means of automated data collection, and with it the increased amounts of data traces available on all levels of our lives. More data means more ways of accidentially disclosing such information, e.g., on a public web page through a system malfunction, and more "needs" of others of getting access to this data; data that was given out voluntarily when using RFID-enabled services.

3 Technical RFID Privacy Mechanisms

The previous sections served to show two things. Firstly, that much of today's discussion on RFID is based on invalid assumptions regarding technical capabilities and societal realities. And secondly, that at the core of the debate, a number of issues are nevertheless threatening substantial privacy values. This section, then, tries to enumerate and analyze the number of proposed technical solutions to those problems. It is important to note that these should not be viewed in isolation, but rather as complementing both each other, as well as corresponding social norms, laws, and regulations.

3.1 Securing Media Access Protocols

As mentioned above, the power asymmetry between reader and tag makes it possible that information sent from reader devices (and to some extend also the tag's reply) can potentially be subject to *eavesdropping* through malicious readers, even at distances larger than the nominal or rogue read range. This is especially critical since it also applies to perfectly legitimate interactions, i.e., when tags only talk to authenticated readers. As pointed out in section 2 above, both the means of RFID for *identification* and *authentication* might threaten an individual's privacy under such circumstances.

Obviously, sending sensitive information from the tag back to the reader might threaten data privacy if overheard. The obvious solution is to encrypt the communication channel between readers and tags. However, this might still allow attackers to learn the ID of the tag (thus threatening location privacy, and possibly data privacy), since many anti-collision protocols send it in the clear on the lower communication levels (see section 1.1 above). Even an otherwise "anonymous" tag ID might in this way threaten location privacy due to the potential for identifying constellations (see section 2 above).

To prevent the transmission of tag IDs in probabilistic protocols (where it is used for silencing already identified tags), tags can instead use temporary session IDs that they choose at random whenever a reader starts a query.

While the ID is then constant over the course of the session (and thus facilitates addressing the tag, e.g., for requesting the real ID's value), it is lost as soon as the reader cuts the field's energy [3].

For deterministic protocols, Weis et al. [36] propose that instead of sending a whole prefix, readers would only send the command "transmit next bit" to the tags. As long as their corresponding bit positions are identical, no collision would occur[20] and the reader would be able to note the common bit prefix incrementally. Once two tags would differ at position i, the reader would just as before use a "select" command to pick a subtree, but instead of sending the complete prefix to the tags, it would send a single bit indicating which part of the subtree should reply next. In order to hide this information from any eavesdropper, the reader XORs it with the previous, error-free bit. As the value of this bit was only sent from the tags to the reader, a malicious reader outside this communication range (but inside the reader's forward channel) will not be able to know the true value of the next selected bit. The tags, on the other hand, know their own ID, and accordingly the bit value at the previously queried position, thus sharing a common secret with the reader that can be exploited for every conflicting bit position.

3.2 Tag Deactivation and the Kill-Command

The most effective privacy protection for RIFD-tagged items is the deactivation of the tag, as it reliably prevents *clandestine scanning* of a tag's *identification* data. In its simplest and most reliable form, this would imply that vendors and manufacturers embed tags only into detachable labels and outer product packaging that can be discarded before use. For tags embedded into the actual product itself (e.g., into the garment of a sweater, or a can of soda), removal of the tag would not be an option – tags would need to be deactivated *in situ*. In standards for item-level tagging of consumer products, compliant tags must implement a "kill"-command [2]. The basic idea is simple: After selling a tagged item to the consumer, the embedded tag is permanently deactivated at checkout. This renders the tag inaccessible to subsequent reader commands and thus prevents any tracking beyond the point of sale.

As simple as the idea sounds, as hard it is to implement in practice. In order to prevent malicious silencing of tags (e.g., for shoplifting), each tag features an individual unlock code that must be sent along by the reader, together with the kill-command, thus significantly increasing data management costs. Also, in situ deactivation itself is for the consumer difficult to verify, as no visible cues would be present. Karjoth and Moskowitz [21] alternatively propose to use scratch-off or peel-off antennas in order to make the silencing process both more visible to consumers and less prone to unnoticed deactivation attacks. Additionally, their solution only removes the wireless communication capabilities but leaves the tag (and its data) intact, thus allowing for a continued

[20] A collision only occurs if two tags send a different bit value.

use of the information in the tag – simply not in the (privacy-violating) automated and unnoticed fashion of regular RFID tags. On the other hand, such a manual approach would increase the burden on the consumer, as one would need to manually disable each tag, while an automated kill-command could be implemented as part of the checkout process. At the same time, however, [32] points out that small businesses such as kiosks might not be able to afford the corresponding equipment, even though they would inevitably sell tagged merchandise (e.g., soda cans or razor blades).

3.3 Access Control

Preserving the benefits of *automated identification* after checkout while at the same time preventing *clandestine scanning* of the tagged data seems to be a contradiction. Yet with proper access control, one could envision that only authorized parties could read out personal RFID tags (i.e., tags containing personal information, or tags affixed to personal items that thus disclose the carrier's location), while queries from rogue readers would simply be ignored.

A simple solution to access control is to obstruct the reader signal by means of a metal mesh or foil that encloses the tag. With the inclusion of RFID tags into passports, a number of vendors begun offering coated sleeves for protecting the passport while not in use. Obviously, this will not be a solution for groceries or clothings. Juels et al. [18] propose a so-called "blocker-tag" that jams tree-based anti-collision protocols, thus making it impossible to read out tags nearby when present. It does so by simply responding to all possible prefixes, thus creating the impression of trillions[21] of tags being present that both hides the real tags present, as well as stalling the reader due to the (apparently) large number of tags to be read out. As it is cheap to manufacture (about the price of a regular tag), it could be even integrated into paper bags, masking any shopping items within. In order to prevent jamming of legitimate read-outs, the authors propose the use of a *privacy-bit* [17] on each regular RFID tag that would be set in the same fashion as the proposed tag deactivation – during checkout. Blocker-tags would then only jam readers that would attempt to read tags with this privacy bit.

A number of authors have proposed cryptographic hashes that hide the real ID of a tag behind a so-called "meta ID," requiring readers to know a certain password (typically the tag's original ID) in order to unlock it again [15]. However, as a single fixed meta ID would not solve the problem of location privacy, i.e., unwanted tracking and profiling, these meta IDs would need to periodically change, e.g., upon each read request. But with an ever changing ID, even legitimate readers might have a hard time figuring out the correct password of a tag in order to unlock it. This implies the need for significant

[21] Fully simulating all possibilities of a, say, 64-bit ID would be actually more than just a few trillions. An (implausibly) fast reader able to read 100'000 tags per second would be busy for over four billion years reading all 2^{64} tags.

data management structures to keep track of one's items and their current meta IDs – a requirement that questions the practicability of such a scheme. Even if one would assume a single password for all of one's personal items (e.g., a smart phone furnishes a key to the supermarket's point-of-sale device during checkout), the associated *key management problem* would still be significant (imagine buying things for other people, or forgetting your phone at home).

3.4 Proxys

The previous paragraph already alluded to a powerful mobile device that could aid consumers with their everyday RFID management, specifically in order to prevent both *clandestine scanning*, as well as *data leakage* during authorized tag readouts. For example, Juel et al.'s blocker tag could equally well be implemented on a mobile phone, allowing more sophisticated blocking strategies, e.g., based on location (don't block readout at home, allow scanning of clothing at your favorite clothing store, etc.) [19]. This could allow RFID systems to still operate *automatically* and use *integrated* and unobtrusive tags.

Flörkemeier et al. [13] additionally propose to incorporate explicit privacy policies into RFID protocols, thus requiring readers to both identify themselves and their operators, as well as explicitly stating the purpose of each tag readout. While not every consumer might be willing or able to afford such an RFID-compliant mobile device, this solution would nevertheless allow independent agencies to audit reader signals and verify that they comply with their stated privacy policies (or, for that matter, that they actually send one).

Proxy approaches are especially interesting in conjunction with public policy proposals that aim at making the tagging and data collection process more transparent. While European legal experts point out that the principles of data protection laws such as collection minimization, transparency, purpose limitation and choice apply equally to RFID [8], U.S. scholars have long since called for voluntary notice and choice requirements for RFID-tagged merchandise [14]. Having legitimate readers transmit detailed privacy policies could significantly improve privacy awareness.

4 Conclusions

RFID technology offers a powerful new way of automating the identification of everyday items. It also opens up new ways of conveniently authenticating ourselves and our devices, facilitating improved services and better security.

However, while RFID technology has come a long way since its inception, it is hard to use it as an all-seeing surveillance infrastructure that many critics fear. Reliability will certainly continue to improve, yet even if one would be able to minimize the rate of false readouts, most envisioned big brother scenarios would still be prohibitively expensive to realize, yet poor in performance. Further advancements in read ranges might actually be unhelpful, as

most item-level applications actually require limited read ranges. And once a service has been implemented using a particular coupling technology, frequency, and antenna design, even rogue readers will not be able to arbitrarily raise the possible read ranges due to the fickle laws of physics governing RFID communication.

Still, behind many of the often contrived examples cited in today's press do lie a number of substantial threats to privacy: the improved means of subtly excerting influence and control through the large amounts of personal data that might be collected – not covertly, but as part of freely chosen services such as loyality programs, recommender systems, or payment schemes; the increased risk for identity theft and credit fraud through poorly implemented RFID authentication systems; and the ever looming desire of society to reuse existing data for secondary purposes, especially when it comes to security (e.g., the war on terror) and safety (e.g., road safety).

Technology can play an important role when it comes to minimizing the risks from malicious attackers, yet it can hardly prevent voluntary data disclosures and self-inflicted surveillance systems. Proper guidelines and laws must complement technical notice and choice solutions in order to protect the rights of consumers to their data. Initiating the public debate on the needs and limits of personal privacy in future smart environments is certainly a welcomed side-effect of today's sometimes sensational RFID coverage.

References

1. Association for Automatic Identification and Mobility. The ROI of privacy invasion. RFID Connections Webzine, January 2004. Available from: `www.aimglobal.org/technologies/rfid/resources/articles/jan04/0401-roispy.htm`.
2. Auto-ID Center/EPCglobal, Cambridge, MA, USA. *860 MHz-930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification*, 2002. Available from: `www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf`.
3. Auto-ID Center/EPCglobal, Cambridge, MA, USA. *900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification*, 2003. Available from: `www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf`.
4. Oliver Berthold, Oliver Günther, and Sarah Spiekermann. Verbraucherängste und Verbraucherschutz. *Wirtschaftsinformatik*, 47(6):1–9, 2005.
5. Stephen A. Brown. *Revolution at the Checkout Counter: The Explosion of the Bar Code*. Wertheim Publications in Industrial Relations. Harvard University Press, Cambridge, MA, USA, 1997.
6. Capgemini. RFID and consumers – what European consumers think about radio frequency identification and the implications for business. Survey, February 2005. Available from: `www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf`.
7. Robyn Curnow. The privacy to pay for VIP status. *CNN.com*, October 6, 2004. Available from: `edition.cnn.com/2004/TECH/10/05/spark.bajabeach`.

8. Resolution on radio frequency identification. 25th International Conference of Data Protection and Privacy Commissioners, November 2003. Available from: www.privacyconference2003.org/commissioners.asp.
9. EPIC – Electronic Privacy Information Center. Radio frequency identification (RFID) systems. The A to Z's of Privacy Website. Available from: www.epic.org/privacy/rfid/.
10. Bastian Fabian, Oliver Günther, and Sarah Spiekermann. Security analysis of the object name service for RFID. In *Proceedings of the 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, July 2005.
11. Thomas Finke and Harald Kelter. Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. BSI White Paper, 2004. Available from: www.bsi.de/fachthem/rfid/Abh_RFID.pdf.
12. Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, Ltd, 2003.
13. Christian Flörkemeier, Roland Schneider, and Marc Langheinrich. Scanning with a purpose – supporting the fair information principles in RFID protocols. In *2nd International Symposium on Ubiquitous Computing Systems (UCS 2004)*, Tokyo, Japan, November 2004.
14. Simson Garfinkel. An RFID bill of rights. *Technology Review*, 105(8):35, October 2002. Available from: www.technologyreview.com/articles/02/10/garfinkel1002.asp.
15. Ari Juels. RFID security and privacy: A research survey. Manuscript. Available from: www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf.
16. Ari Juels. Attack on a cryptographic RFID device. Guest Column in RFID Journal, February 28, 2005. Available from: www.rfidjournal.com/article/articleview/1415/1/39/.
17. Ari Juels. RFID privacy: A tecnical primer for the non-technical reader. In Katherine Strandburg and Daniela Stan Raicu, editors, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Springer, 2005. Available from: www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/DePaul23Feb05Draft.pdf.
18. Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In Sushil Jajodia, Vijay Atluri, and Trent Jaeger, editors, *Proceedings of the 10th ACM Conference on Computer and Communication Security*, pages 103–111, Washington, D.C., USA, 2003. ACM Press. Available from: portal.acm.org/citation.cfm?id=948126&coll=Portal.
19. Ari Juels, Paul Syverson, and Dan Bailey. High-power proxies for enhancing RFID privacy and utility. Workshop on Privacy Enhancing Technologies (PET 2005), May 2005.
20. Andrew Kantor. Tiny transmitters give retailers, privacy advocates goosebumps. USAToday.com – CyberSpeak, December 19, 2003.
21. Günter Karjoth and Paul A. Moskowitz. Disabling RFID tags with visible confirmation: clipped tags are silenced. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *WPES*, pages 27–30. ACM, 2005.
22. Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *Conference on Security and Privacy for Emerging*

Areas in Communication Networks – SecureComm 2005. IEEE, September 2005. Available from: eprint.iacr.org/2005/052.pdf.
23. Brian Krebs. Leaving Las Vegas: So long DefCon and Blackhat. washingtonpost.com Weblog, August 2005. Available from: blogs.washingtonpost.com/securityfix/2005/08/both_black_hat_.html.
24. Matthias Lampe, Christian Flörkemeier, and Stephan Haller. Einführung in die RFID-Technologie. In Elgar Fleisch and Friedemann Mattern, editors, *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*, pages 69–86. Springer-Verlag, 2005. Available from: www.vs.inf.ethz.ch/publ/papers/mlampe-rfid-2005.pdf.
25. Ching Law, Kayi Lee, and Kai-Yeung Siu. Efficient memoryless protocol for tag identification (extended abstract). In *Proceedings of the Fourth International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pages 75–84. ACM Press, 2000. Available from: portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal.
26. John Lettice. Face and fingerprints swiped in Dutch biometric passport crack. *The Register*, January 30, 2006. Available from: www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/.
27. MIT RFID Privacy Workshop, November 15, 2003. Available from: www.rfidprivacy.us.
28. Mary Stuart Relfe. *When Your Money Fails*. League of Prayer, Montgomery, AL, USA, January 1981.
29. Mark Roberti. Big brother's enemy. RFID Journal, July 2003. Available from: www.rfidjournal.com/article/articleview/509/1/1/.
30. Chana R. Schoenberger. The internet of things. *Forbes Magazine*, 2002(6), March 2002. Available from: www.forbes.com/technology/forbes/2002/0318/155.html.
31. Spychips.org. Two U.S. employees injected with RFID microchips at company request. Press Release, February 2006. Available from: www.spychips.com/press-releases/us-employees-verichipped.html.
32. Ross Stapleton-Gray. Scanning the horizon: A skeptical view of RFIDs on the shelves, July 2005. Available from: www.rfidprivacy.us/2003/papers/stapleton-gray3.pdf.
33. Roy Want. The magic of RFID. *ACM Queue*, 2(7):41–48, October 2004. Available from: www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=216.
34. Roy Want. RFID – a key to automating everything. *Scientific American*, 290(1):46–55, January 2004.
35. Stephen A. Weis. *Security and Privacy in Radio-Frequency Identification Devices*. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, May 2003. Available from: theory.lcs.mit.edu/~sweis/.
36. Stephen A. Weis, Sanjay E. Sarma, Ron L. Rivest, and Daniel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *Security in Pervasive Computing: First International Conference*, volume 2802 of *LNCS*, pages 201–212, Boppard, Germany, 2003. Springer-Verlag. Available from: www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2802.
37. Markus Zeidler. RFID: Der Schnüffelchip im Joghurtbecher. Monitor-Magazin, January 8, 2003. Available from: www.wdr.de/tv/monitor/beitrag.phtml?bid=554&sid=108.