CHAPTER 14

Killing, Recoding, and Beyond

"Dead men tell no tales," and dead tags don't talk. This is the logic behind RFID tag "killing," a proposal for enhancing consumer privacy that has received wide attention. In tag killing, RFID tags are rendered permanently inoperative by use of a special command. Killing is envisioned as an answer to privacy concerns over ``item-level tagging" in the retail setting, in which each item is provided with a unique RFID tag. The logic behind tag killing is simple: by destroying the RFID at point of sale, the item can no longer be tracked via RFID after it has passed to the consumer. At first

glance, RFID tag killing appears to be an inexpensive way to address privacy concerns with RFID deployment. Unfortunately, there is more to tag killing than meets the eye.

Tag killing has received so much attention because it has become clear that privacy in item-level tagging will be a hot-button issue in consumer acceptance of RFID. Privacy issues in item-level tagging include the possibility of tracking individuals by a unique tag or a collection of tags.

Today, one of the most influential bodies in supply chain and retail RFID is EPCglobal, Inc., a joint venture of the Uniform Code Council and EAN International, two primary bodies that administer current commercial bar codes. Supported by WalMart, among others, EPCglobal publishes specifications for RFID tags and defines mechanisms for use of RFID data. Tag killing has been enshrined by EPCglobal in its specifications for RFID tags, all of which support a password-protected kill command.

Unfortunately, there are several issues with kill commands. First, killing tags prevents all post-point-of-sale uses for RFID tag information. These

uses are expected to become more important as the use of RFID tags on retail items spreads.

Second, RFIDs used for rental and borrowing, such as in libraries, should not be killed, as the RFID must be used to return the item. This is particularly problematic because these applications pose some of the clearest privacy risks. Video rental records and library patron records are protected by both state and federal law. If it is possible to scan someone with an RFID reader and determine what videos or books they are reading, the spirit of these laws can be completely circumvented.

To address these issues, we suggest “recoding” as an additional tool for RFID privacy. In recoding, a tag is overwritten with a new ID number when it changes hands. Without knowledge of the map from the old ID number to the new ID, it is impossible to link sightings of the item from before and after recoding. Recoding may occur at point of sale, or within the supply chain when an item passes from one organization to another. For example, a retailer might recode RFID tags on items received from a distributor so that

other parties cannot determine how many items were bought of each type; these new RFID tag IDs might also point to a private database of the retailer.

We can use recoding as a tool to build RFID "infomediaries." An infomediary is a trusted third party that mediates requests for information about an RFID tag; for example, the infomediary might only allow requests that match a specified privacy policy. The use of an infomediary makes possible post-point-of-sale RFID applications while lessening privacy concerns.

In addition, rental stores and libraries can act as their own infomediaries and control access to information about their items. Recoding can also be used to remove information from an RFID tag that is not needed for post-point-of-sale applications.

Both killing and recoding raise infrastructure issues that need to be solved before they can become viable privacy protections. In particular, only authorized parties, such as a retailer, should be able to kill or recode tags. How is this restriction enforced? We discuss the "kill passwords" and write passwords in current generation RFID tags, and ways to distribute these passwords to authorized retailers.

In addition, killing and recoding both require an RFID reader, but readers are not currently widespread in retail settings. More importantly, some retailers will see less benefit from installing RFID readers than manufacturers or distributors. Therefore we would expect RFID readers to be much less widespread in retail stores, which is a problem because readers are needed at the point of sale to perform killing or recoding. We discuss several approaches to this problem, such as legislating that every retailer install an appropriate RFID reader for killing or recoding tags.

In the end, while both are important tools, neither killing nor recoding is the final answer in RFID privacy. We close by identifying privacy issues not addressed by either killing or recoding, and motivate the need to go "beyond" these two mechanisms.

14.2 RFID Recoding and Infomediaries

We first enumerate the post-sale applications prevented by RFID tag killing, which justifies considering other options such as recoding. Then we

show how recoding RFID tags can work with the RFID processing framework proposed by EPCglobal to create “infomediaries.”

14.2.1. Applications Prevented by Killing

Killing RFID tags at point of sale prevents several beneficial applications in the short, medium, and long term. In the short term, RFID tag killing prevents tags from being used to manage returns and recalls. Many stores would find it easier to manage returns of items by keeping a database of tag IDs from items sold. The store might find it useful to scan the item and compare it to the database. In item recall, some have suggested a consumer might bring an item to an RFID reader and quickly learn if its tag matches a database of recalled items. While these applications could be enabled by optical bar code scanning, it is believed that RFID technology will reduce the overhead needed to gather this data and check items against the database.

Unfortunately, these schemes for product return and recalls are incompatible with killing of RFID tags. We note, however, that many of these applicationss do not require RFID tags, but only unique identifiers for each

item. If it were possible to print bar code labels containing EPC codes, which are unique to each item instance, those labels could be used for recall and return.

One of the short-to-medium term applications enabled by RFID item tagging, and not possible with optical bar code scanning, is automatic sorting of items for recycling. Different materials require different recycling processes. Currently, items placed for recycling must be sorted by hand or semi-auotmatically, which greatly increases the cost of recycling and limits its use. By encoding the composition of an item onto its RFID tag, the vision is that sorting can be made fully automatic[1]. This vision is only possible if tags remain unkilled at point of sale.

In the longer term, item-level RFID tagging may enable a wide range of applications post-sale. Nokia recently released a kit that allows certain cell phone models to read RFID tags; combined with item-level tagging, this could provide a way for people to scan an item and be automatically directed

---

[1] Saar, Steven. "RFID System Implementations for Environmental Applications." Online at http://www.princeton.edu/~vmthomas/recyclebox.html

to further information about that item. Washing machines equipped with RFID readers could read RFID tags on clothes containing wash instructions. Refrigerators could detect spoiled food and warn their owners. An article by Want describes some of these applications[2]. At Microsoft Research, the Advanced User Resource Annotation (AURA) project led by Marc Smith is exploring the space of possible applications enabled by end-user scanning of tags[3].

Some of these applications are more speculative than others. The privacy risks, however, are not at all speculative. We suggest a principle for evaluating RFID architectures: we should not allow speculations about the potential applications of tomorrow to justify definite degradations of privacy today. Put another way, it is better to design architectures that "fail private." We also note that some applications may not need the full information about an item; for example, recycling applications need only the composition of the

---

[2] Want, Roy. "RFID: A Key to Automating Everything." Scientific American, January 2004.

[3] Smith, Marc, and Davenport, Duncan, and Hwa,Howard. "AURA: A mobile platform for object and location annotation", in Ubicomp 2003

item, not its specific serial number. Recoding offers one way to limit the amount of information available from an item's RFID tag to only the minimum needed.

14.2.2. Recoding and Electronic Product Codes

Manufacturer ID	Item Type ID	Serial Number

Assigned by EPCglobal Assigned by Manufacturer

Figure 1. The format of an Electronic Product Code (EPC).

Electronic Product Codes (EPCs), like Universal Product Codes (UPCs) before them, are fundamentally two-part codes. The first part of the code is a unique identifier of a manufacturer. This unique identifier is assigned by EPCglobal, which is the entity responsible for maintaining the EPC namespace. The second part of the code is an identifier for a product, assigned by

the manufacturer. A key innovation of the EPC, as compared to the UPC and similar codes, is that the second part of the EPC code also includes a unique identifier for each instance of each product.

Each field of an EPC, however, provides information that might be used to compromise privacy. The first field is the manufacturer's unique ID, or, in EPCglobal parlance, the “EPC Manager Number.” Knowing this field alone provides only a coarse-grained knowledge (e.g. "this is an item manufactured by Tom's of Maine"). Knowing both the first and second fields gives the manufacturer, plus the product identifier, which is enough to determine a specific type of item ("12 oz. can of Coke Classic"). Knowing those two fields, plus the unique serial number, would allow for tracking over time.

It is important to understand that EPCs will complement and expand on existing product codes such as UPCs currently used in product bar coding; item-level EPCs will in all likelihood be based on previously-assigned UPCs. There are numerous commercial sources of information mapping UPCs to product names and other information. Google even offers a free, if crude,

equivalent. Product codes--both the EPC, and its non-RFID-oriented predecessors--are supposed to be readily used as indices to product information, with little regard for privacy interests.

One could imagine several different recoding schemes, intended to frustrate or confuse such mappings. For example, one could zero out the unique serial number on an EPC, which reduces the EPC to little more than a UPC: if the tag is read, one can understand who the manufacturer is, and what the product is, but cannot make any meaningful inferences that would rely on tracking a specific instantiation of that product.

The recoding scheme with the greatest potential for privacy protection is one in which all the fields are remapped: the original manufacturer ID is changed to that of an entity which administers recoding services, and this administrator then assigns a unique serial number to be contained in the other fields. The administrator retains an association of the new EPC and the original, so that knowing the former one could retrieve the latter, if permitted. We call such an administrator an “infomediary.”

An infomediary has an ability to apply access controls, and govern who can know what about whom. For example, a consumer might have an item recoded at point of sale with an EPC that lists the infomediary as the "manufacturer ID," together with a serial number assigned by the infomediary. Now, if someone reads the tag and wishes to know what the item is, that person must ask the infomediary. The infomediary, in turn, consults the consumer's privacy policy before responding to the request – for example, the infomediary may allow requests for information on clothing RFID tags from the consumer's washing machine, but deny requests from unknown RFID readers.

In rental or borrowing applications, the rental store or library could act as its own infomediary. Before item checkout, the RFID tag contains an EPC that identifies the item. At item checkout, the RFID tag is recoded with a new random identifier and the store as the "Manufacturer ID." Then, when the item is read, any third-party RFID reader must query the store to learn anything useful. Readers belonging to the store, such as those used for item

check-in, can be permitted to access the store database. Requests from third-party readers can be denied.

An infomediary could be implemented within the context of the EPC Object Name Service (ONS) proposed by EPCglobal. The ONS offers a service that maps EPC manufacturer IDs to URLs; these URLs in turn lead to web sites set up by the manufacturer that provide more information about the item given its type ID and unique serial number. The ONS is currently being being built by VeriSign, Inc, a company that has previous experience running a Certificate Authority for Web public-key infrastructure and in managing the Domain Name Service. Once the ONS is built, an infomediary could be implemented simply by registering its specific manufacturer ID with the ONS and creating a web site to store privacy policies and handle the resulting traffic. Therefore EPC privacy infomediaries appear feasible in the near term, as long as RFID tags support recoding.

14.3 INFRASTRUCTURE ISSUES

14.3.1. Protecting the Kill Switch

In architectures that use killing, some mechanism must be used to prevent unauthorized killing of RFID tags. Current EPCglobal specifications state that a password will be used. In Class 1 915MHz tags, this password is 8 bits, while in Class 0 13.56MHz and 915MHz tags, the password is 24 bits. A tag will not honor a kill command without the proper password, and passwords are unique to each tag[4].

This raises the question of how passwords are provisioned to legitimate RFID equipment at point of sale. Without the passwords, tags cannot be easily killed, and so we lose the privacy benefits of tag killing. On the other hand, if passwords are easy to guess or poorly protected, adversaries might abuse the kill feature and kill tags before point of sale.

---

[4] EPCglobal, Inc. Version 1.0 EPC Tag Specifications. Available online at http://www.epcglobalinc.org/standards_technology/specifications.html

Perhaps the most straightforward answer is to have a central database mapping RFID tag IDs to kill passwords, perhaps maintained by the RFID tag manufacturer. Unfortunately, this database becomes a single point of failure: if ever compromised by an adversary, all tags in the database become vulnerable to malicious killing.

As a simple alternative, we propose “two-part” RFID tags. The first part of the RFID tag reveals the kill command for the entire tag to any reader, but can itself be deactivated without a password. When a manufacturer takes delivery of tagged items, it reads the first part to obtain the tag kill command and places that into its own private database, then deactivates the first part. Later, when the manufacturer passes items to a distributor, or when a distributor passes items to a retailer, it also passes a database mapping RFID tag IDs to kill passwords; these databases can be managed by bilateral agreements.

14.3.2. Recoding, Rewriteable Tags, and Vandalism

Recoding requires rewriteable tags, but the ability to rewrite a tag must be protected. Otherwise, RFID tag "vandalism" becomes possible – a vandal can change the data on an RFID tag to make an item appear to be something it is not, or simply erase the tag entirely. Vandalism might be performed to deny service to legitimate users, or there might be some financial motive involved.

While RFID tag vandalism has not yet been reported, we suspect it is only a matter of time. Environments such as libraries already suffer attacks from fairly sophisticated vandals. With respect to financial motives, scams have already appeared that switch optical bar code labels. For example, Home Depot suffered nearly half a million dollars in losses from a group of thieves that created bar code labels for low-cost items, pasted them on top of high-cost items' labels, bought the items at a discount, and then returned the item for the full price. In the RFID setting, we could expect to see a quick "cloning" of other items found in the same store, in which a thief would read

a code off a cheap (but similar) product, then overwrite the tag of a more expensive product.

Many of today's RFID tags employ a "write then lock" architecture, in which the tag data can be written an unlimited number of times and then irrevocably "locked." After locking, the data on the tag cannot be modified or erased. Unfortunately, this irrevocable lock does not work for recoding, because the data on the RFID tag must be modified. Instead, some kind of write password will need to be employed; the password can then be provisioned as we have described for kill passwords.

14.3.3. The ``Sub-Threshold" Retailer

Killing or recoding a tag requires both an RFID reader and the infrastructure to provision it with the appropriate passwords as we have discussed. Both readers and infrastructure cost money. Even though we have discussed ways of avoiding a centralized password repository, creating this infrastructure is still a significant investment.

Not all retail outlets may make the investment necessary to enable killing at point of sale, an observation made independently by Hughes[5]. We call a retail outlet that is unable or unwilling to provide RFID tag killing a "sub-threshold" retailer. For example, a small family-owned convenience store may decide that an RFID reader is too expensive for the in-store benefit it provides.

The problem with sub-threshold retailers is that they allow for RFID tags to "leak" into the post-sale environment. Because tags are applied at manufacture time, sub-threshold retailers may take delivery of items with live RFID tags. Neither the sub-threshold retailer nor the ordinary customer is capable of even detecting the presence of tags, let alone killing them. As a result, items may be sold to a customer with live RFID tags, even if the recommended best practice is that all tags must be killed at point of sale.

---

[5] Hughes, Sandy. "RFID and Privacy in the Supply Chain – A Team Effort for Consumer Trust," this volume.

14.3.4. Who Pays?

The case of the sub-threshold retailer illustrates a problem with both RFID tag killing and recoding infrastructure: who will pay? A large part of the cost falls on the end retailer, but the retailer has the least incentive to deploy RFID equipment. Consumers are unlikely to have their own RFID readers in the foreseeable future, and so it looks likely that many goods will be sold without an RFID reader present. Therefore, it becomes difficult to depend on killing or recoding RFID tags at point of sale as a privacy mechanism.

One way to address this would be to legislate that all retailers must possess appropriate RFID equipment to perform killing or recoding. One advantage of this approach is that auditing compliance is fairly straightforward. A single visit to a store suffices to check whether the infrastructure is in place. In addition, once a store has bought the necessary equipment, it can be continuously used for tag killing or recoding. While several pieces of legislation concerning RFID are under consideration in several states, including California and Utah, we are not aware of any that explicitly treats the issue of

readers in the retail setting. Unfortunately, such legislation is likely to be politically problematic, and the cost of such infrastructure would almost certainly be passed directly to consumers.

Another approach, for the case of RFID tag killing, would be to shift the site of killing to the distributor. Before delivering items to a retailer without the means to kill tags, the distributor could simply kill the RFID tags en masse. This could be required by legislation or codified as part of industry best practices. Again, this can be audited for compliance fairly easily; anyone with an RFID reader could check for the presence of unkilled tags.

As a final alternative for tag killing, we could ask for tags that can be physically destroyed by consumers. Peter de Jager notes that physical destruction has the major advantage that anyone can be convinced that the tag is really destroyed[6]. With approaches that require the use of RFID readers to kill or recode tags, it is difficult for most people to verify that the tag is in the

---

[6] de Jager, Peter. "Store Experiments on Human Subjects in Secret Using Alien Technology – or – How to Make Consumers Stop Worrying and Love The Bomb," this volume.

correct state – for example, that the tag is "all dead," as opposed to "mostly dead" and possibly able to be awakened later.

14.3 BEYOND KILLING AND RECODING

There are several take-home points from our analysis. First, killing alone is not enough, and new mechanisms are needed for building privacy-preserving RFID architectures. Killing is not sufficient for borrowing applications, or for post-sale applications such as recycling.

Second, recoding is a useful tool for building privacy-protecting RFID architectures. Recoding allows "excess" information to be removed from a tag at point of sale, and for the construction of EPC infomediaries. Recoding and infomediaries can produce privacy-friendly architectures for applications that are not well served by tag killing.

Finally, both killing and recoding raise infrastructure issues. While the solutions to these issues may be simple, these issues must still be resolved before these mechanisms can become effective. Finding a satisfactory

solution will require both policy tools, such as legislation, and good technical design.

Even after the infrastructure issues have been solved, however, there are still privacy issues that will not be addressed by killing or recoding. Live RFID tags of today's generation have static identifiers between recodings. Therefore, it is possible to track individuals by linking different sightings of the same RFID tag identifier. Until the RFID tag is recoded, the movements of the tag can be registered and correlated by different readers.

Even if individual tags change their identifiers, an individual may carry multiple different RFID tags. This "constellation" of RFID tags can uniquely identify an individual. Unless many of the tags change their identifiers at the same time, recording readings of constellations that share many tags may give enough information to track an individual.

In general, static identifiers on RFID tags, combined with no access control (such as a read password) for tags, enable tracking invasions of privacy. In addition, once sightings of these identifiers have been placed in a

database, controlling the inferences that may be drawn from that database raises a set of database privacy issues by itself.

Dealing with these privacy issues will require measures that go beyond killing and recoding. Juels, elsewhere in this volume, outlines current and future technical solutions for preventing tracking attacks[7]. There is a rich literature on database privacy issues, and these issues are notoriously difficult to deal with. Killing and recoding are just the first steps.

[7] Juels, Ari. "Technical Approaches to RFID Privacy," this volume.