NAME:

STUDENT NUMBER:

TITLE: The privacy risks of RFID

Introduce the topic.

- Radio frequency identification, RFID for short, is making an appearance in almost every aspect of our daily lives. It is present in a lot of products and has also made its way into our phones.
- RFID is mostly used to keep track of products in factories and for shipping purposes. RFID could also be used for tracking and identifying someone.
- RFID tags can be read from a distance and most of them do not even need energy because the reader provides that for them. This means that, once these tags are rolled out, they will be alive for ever.

Describe the types of privacy that are relevant for your topic. Use the Finn, Wright, and Friedewald's Types of Privacy as explained in A Typology of Privacy, Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski and Maša Galič, pp. 7-19.

- The main issue with RFID is that each tag has a unique identifier. This means that all the tags in the world can be uniquely identified and could thus be used to track us if we carry them with us. This means a violation of privacy of behavior and action, privacy of location and space and privacy of association.
- The new ePassports with an RFID chip contain fingerprint data of the user. This application of RFID threatens the privacy of the person as it is a body characteristic.

Describe the privacy threats that are posed by your topic using Daniel J. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3 (Jan., 2006), pp. 477-564.

- RFID could be used for surveillance purposes by methods already stated above.
- Insecurity can also be applied on RFID. Once rolled out, RFID chips have an almost infinite life due to their lack of battery. This means that data (that might not be deletable) that is stored upon such a chip will be stored forever. This also applies for encrypted data, if the encryption gets broken, the data on such a chip is no longer secure.
- Factories use RFID chips on their products to track them through their factory. Shop owners use them to prevent theft. These RFID tags are already in our clothing. They are now almost every time destroyed when buying the clothes but the RFID tags could, after buying, also be (secondary) used for tracking purposes or for servicing personal advertisements.
- Exclusion applies to RFID chips. Information that is stored on an RFID chip can not be easily accessed or updated by a normal user. If personal data is stored upon an RFID chip, the user should be able to see what kind of data is stored and update it.

Analyse to what extent the laws of identity relate to the problem using Cameron, Kim. "The Laws of Identity." Microsoft Corporation (2005).

- With RFID enabled devices and tags all around us these days, the first law of identity proposed by Kim Cameron can already be applied. RFID tags can be read from a distance without the user's consent. The user is thus not in control over what data it gives to what authorities.
- Most RFID tags contain a unique identifier that can be read with an RFID reader. This can be done by anyone without the user knowing that it is happening. This clashes with the justifiable law proposed by Kim Cameron.
- RFID chips emit an omni-directional public beacon (as stated in the paper). The RFID tag can be used to identify someone and thus clashes with law four.

Argue whether or not personal data is being processed. Explain what basic data protection rules apply to your topic. Explain if the special regime for sensitive data or research or statistical purposes is applicable. If so, what is the effect compared to the basic data protection rules apply to all personal data processing.

- The data on the RFID tags vary. Tags in clothing for example, are only used by the retailers to prevent theft. On the other hand, there are also tags in our passports and in our mobile phones, these can actually contain personal data. For all tags that contain personal data, the basic data protection rules apply. This is the case with, for example, a bankcard or passport.
- Tags do not need to contain personal data for them to be a privacy thread. Tags that just contain a serial number for example, can be used to track us and thus can also be used to process personal data. For example, if someone bought a watch that contains an RFID tag with a serial number. That watch's tag could also be used as a serial number for the wearer. In this case, the basic protection rules would also apply.

Describe the functioning of a PET that will solve (part of) the problem using the interdisciplinary vocabulary as described by Andreas Pfitzmann and Marit Hansen, A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, pp 1-35.

- An RFID kill function could allow people to deactivate RFID tags just as is done in stores now.
- Make the reading of an RFID tag physically restricted (by an on/off switch). This means that we decrease the linkability of RFID tags because unintentional readouts of the tag become impossible. Also the detectability decreases because the tag is not emitting data when it is physically turned off.
- Make readings of an RFID tag impossible except when the user has authenticated. This way a tag is shutdown but can be revived by a user with a password. Before the tag gets read out, a user actively takes a decision on whether the tag may be read. This means that the linkability of a tag decreases but the observability remains the same (for authenticating purposes, challenge-response).

Analyse to what extent that PET solves the problem en to what extent the PET introduces new privacy and identity problems.

- The deactivation of RFID tags has to be done with a certain password because otherwise, anyone could just walk up and destroy RFID tags. This password needs to be kept secure so this solution does not necessarily cause new privacy and identity problems but rather a security problem.
- Authenticating via a password to the tag also relies on a good password. The privacy of the user thus relies upon the strength of the password. To implement this technology, not only does the tag need to be rewritable (when a password gets stolen), it also needs to be kept secret.

Make recommendations with regard to behavioural adaptations and technical design choices that result in a privacy and identity management positive environment.

- An RFID tag should have some kind of shutdown mechanism and thus let the user control on whether it is on or off. This way unauthorized access to the tag is prevented.
- People should be made aware of RFID tags in their products. This can be achieved by creating stickers to put on products that contain RFID tags.
- RFID tags that are not actively being used anymore (such as the ones that are used in factories, after they leave the production area) should be instantly deactivated. This prevents secondary use, for example, tracking of the tags outside their intended area.

Conclusion

- RFID is a great technology and brings with it a lot of nice features but we should be careful when using it.
- When applying RFID in some sort of situation. The privacy risks should be made aware and avoided as much as possible.

Bibliography

- Beugelsdijk, R. (2006). RFID, Veelbelovend of onverantwoord? Bijdrage aan de maatschappelijke discussie over RFID (CBP).
- Hoekman, J., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R. W.. Crossing Borders: Security and Privacy Issues of the European e-Passport.
- Spiekermann S., Evdokimov S.. Privacy Enhancing Technologies for RFID – A Critical State-of-the-Art Report
- Information Commissioner's Office (2006). Data Protection Technical Guidance Radio Frequency Identification.
- Hennig, J. E., Ladkin, P. B., Sieker, B. (2004). Privacy Enhancing Technology Concepts for RFID Technology Scrutinised.