U.S. Federal Trade Commission
Staff Comments to the European Commission on its
"Draft Recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID)."

The staff of the United States Federal Trade Commission (FTC)[1] respectfully submits these comments to the European Commission (EC) in response to its "Draft Recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID)." The FTC staff appreciates the continuing opportunity to engage in this important dialogue with the EC on how to address consumer privacy issues in the context of such emerging technologies. These comments will provide a brief overview of the FTC's multi-faceted approach to protecting consumer privacy through

account differences in the size and complexity of the range of companies that we regulate, as well as the sensitivity of the information at stake. It also allows us to respond to developments related to new and emerging technologies without the need for technology-specific regulation. The focus of this approach is on assessing risks to consumer information throughout its lifecycle – from collection to storage to transmission to

medium-sized businesses in developing information security plans.[6] The FTC has long supported meaningful industry self-regulation, particularly when it comes to rapidly evolving technologies and business practices where industry is in a position to anticipate how a particular technology will be deployed and how it might affect consumers.[7]

The FTC also addresses emerging issues through public workshops. For example, in 2004 the FTC held a workshop devoted to RFID, "Radio Frequency Identification: Applications and Implications for Consumers." FTC staff subsequently published a workshop report that analyzed the present and potential uses of RFID and the relevant benefits and countervailing concerns associated with those applications. The report, which was issued in 2005, also offered some specific recommendations for industry conduct involving consumer uses of RFID.[8]

Comments on the EC's Draft Recommendation

Article 3: Privacy and Data Protection measures

Article 3.1: Before an RFID application is implemented, the RFID application operators should conduct, individually or jointly within a common value chain, a privacy impact assessment to determine what implications its implementation could raise for privacy and the protection of personal data, and whether the application could be used to monitor an individual.

Article 3.2: The level of detail of the assessment should be proportionate to the risks associated with the particular RFID application. The assessment should comply with good practice frameworks to be established in a transparent way in partnership with all relevant stakeholders, and in consultation of the relevant supervisory data protection authorities.

The staff of the FTC encourages companies deploying RFID technology to assess the potential risks to consumer information and to take reasonable steps to mitigate the identified risks. In fact, this is the approach we recommend in our data security guidance for business, "Protecting Personal Information: A Guide for Business," and the approach that underlies our enforcement in the data security area.[9] The EC's Draft Recommendation takes a similar risk-based approach with its suggestion that RFID application operators conduct a privacy impact assessment and that "[t]he level of detail of the assessment should be proportionate to the risks associated with the particular RFID application." We agree that a risk-based approach is

---

[6] The booklet and the online tutorial are available at http://www.ftc.gov/infosecurity/.

[7] For example, the FTC currently is engaged in an initiative to encourage the development of self-regulation in the evolving area of online behavioral advertising. *See* http://www.ftc.gov/opa/2007/12/principles.shtm.

[8] Information about both the FTC RFID workshop and staff report is available at http://www.ftc.gov/bcp/workshops/rfid/index.shtm. Although the FTC has not developed consumer outreach materials specific to RFID, we are following developments in the technology and will consider outreach to consumers as more consumer-facing RFID applications are deployed.

[9] In cases where companies fail to take reasonable steps to protect consumer privacy, and that failure results in harm to consumers, the FTC can bring an enforcement action under its Section 5 unfairness authority.

Article 5: Information on RFID use

Article 5.1: Where RFID applications are implemented in public places, RFID application operators should make publicly available a written comprehensible policy governing the use of their RFID application…

As noted above, the FTC has encouraged companies to publicize to consumers in a privacy statement how their information is being collected and used. We believe that this serves an important role in making consumers aware of potential issues and risks to their personal information and allows them to make informed choices to protect themselves. In the context of an emerging technology such as RFID, statements about how the technology works and what personal information it collects are especially important to dispel any consumer fears about the technology and to inform consumers about what they can do to protect themselves from inappropriate uses of the technology.

Article 6: Information security risk management

Article 6.1: Member States should encourage RFID application operators to establish information security management according to state-of-the-art techniques, based on effective risk management in order to ensure appropriate technical and organizational measures related to the assessed risks. The security threats, and the corresponding security measures, should be understood as covering all components and interfaces of the RFID application.

As the FTC staff noted in its 2005 RFID Workshop report, there was a general consensus at the workshop that many of the privacy concerns associated with RFID technology implicate broader database security issues. Although RFID may facilitate more data collection, the real issue is ensuring that there are appropriate safeguards for that data, as well as for data linked to RFID data. Similarly, the FTC staff encourages itsCID 0.0foc0.0allo The-0003 Tc -0.0003 Tw -27.74 -2749n e

With respect to RFID, the FTC encourages industry efforts to raise consumer awareness and understanding of the technology. Because of the danger of consumer confusion potentially resulting from a proliferation of symbols indicating the presence of an RFID tag, however, the FTC staff agrees with the EC's recommendation for a "harmonised" approach in this area.

Article 7.3: (a) Where a RFID appnu55r

staff particularly supports the attention given in this section to small and medium-sized enterprises that might not be aware of the potential benefits of using RFID technology.

Conclusion

The staff of the FTC appreciates the careful consideration of consumer privacy and data security issues related to RFID applications, as well as the willingness to engage with stakeholders outside of Europe on these important issues. The FTC staff supports the EC's risk-based approach to addressing potential consumer privacy and data security issues related to the use of RFID technology. The FTC staff also agrees with the EC that there is a need to raise consumer awareness about RFID technology, in order to enhance consumer trust and to give consumers the tools to protect themselves from the risk of misuse of their information. Given the current stage of deployment of consumen. Given t(nt o give0.0003 Tc -0.0028 TTu-1.need tor-facology.)Ta