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 vigorous law enforcement, consumer and industry awareness initiatives, and encouraging effective industry self-regulation. The comments also will describe our experience with RFID issues and address the specific articles set forth in the EC's Draft Recommendation.

Introduction: The FTC's approach to protecting consumer privacy

The FTC is a general jurisdiction consumer protection agency with responsibility for enforcing national consumer protection laws, including laws related to the privacy and security of individuals' information. Although the FTC enforces a number of sector-specific privacy and data security laws, its primary authority derives from its general consumer protection statute, Section 5 of the FTC Act.[2] Under Section 5, the FTC has broad authority to challenge unfair or deceptive acts or practices in or affecting commerce. Because of the flexible nature of this authority, the FTC frequently has found itself on the forefront of privacy and other consumer issues arising from emerging technologies. The FTC has used its Section 5 authority to address many different types of harmful practices related to consumer privacy, including deceptive claims that companies have made about their privacy practices or the level of security they employ to protect consumer data. The FTC has also brought cases under its unfairness authority challenging privacy and data security practices that caused or were likely to cause harm to consumers not outweighed by benefits to consumers or competition.

Although the FTC's legal authority in the privacy area is broad and flexible, we apply a consistent standard designed to protect consumer privacy and to send clear signals to industry: we expect companies to take reasonable steps to address risks to the security and privacy of individuals' information.[3] This flexible, process-oriented approach allows us to take into

[1] These comments represent the views of the staff of the FTC and not necessarily the official views of the FTC or any individual commissioner.

[2] 15 U.S.C. §§ 41-57.

[3] The FTC's Safeguards Rule, 16 C.F.R. Part 314, which applies to financial institutions under the FTC's jurisdiction, requires the implementation of a comprehensive written information security program, a risk assessment that addresses key areas of a business's operations (employee training and oversight; information

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 disposal – and then on adopting safeguards that are reasonable and appropriate to mitigate the identified risks. A failure to take such appropriate steps to address risks to consumer information could result in a Section 5 action by the FTC – either under its deception authority (where a company makes promises about privacy or data security practices that it fails to keep) or under its unfairness authority (where the failure to take reasonable steps to protect consumer privacy results in actual or likely harm).[4]

In addition to its vigorous law enforcement, the FTC also places a high priority on outreach and education. We inform consumers about emerging threats and strategies for protecting themselves from harm using a wide variety of media, from printed materials to our well-known OnGuard Online website for consumers.[5] OnGuard Online includes an extensive online tutorial for consumers divided into sections such as wireless security, phishing, social networking, and online shopping. We also inform industry of their obligations under the law and encourage responsible self-regulatory practices. For example, the FTC has developed guidance, entitled "Protecting Personal Information: A Guide for Business," designed to assist small and

---

systems, including network and software design, as well as information processing, transmission, storage, and disposal; and incident response), and the development and implementation of safeguards to mitigate identified risks. The Rule also imposes a requirement that the financial institution periodically reassess the effectiveness of the security program, update the program as appropriate, and oversee service providers. Although the Rule only applies directly to financial institutions, the Rule's general approach is instructive in the FTC's assessment of the reasonableness of other companies' privacy and data security practices. *See also* Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.* (requiring consumer reporting agencies to have reasonable policies and procedures to prevent misuse of consumer report information).

[4] *See In the Matter of The TJX Companies*, FTC File No. 0723055 (proposed settlement posted for public comment Mar. 27, 2008); *In the Matter of Reed Elsevier Inc. and Seisint Inc.*, FTC File No. 0523094 (proposed settlement posted for public comment Mar. 27, 2008); *United States v. ValueClick, Inc.*, No. CV08-01711 (C.D. Ca. Mar. 13, 2008); *In the Matter of Goal Financial, LLC*, FTC File No. 0723013 (proposed settlement posted for public comment Mar. 4, 2008); *In the Matter of Life is Good, Inc.*, FTC File No. 0723046 (proposed settlement posted for public comment Jan. 17, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 3, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (Jun. 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (Jul. 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002). Information about these actions, as well as additional actions relating to consumer privacy issues, are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

[5] Information about OnGuard Online and other FTC consumer education initiatives about computer security is available at http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm.

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.

appropriate in this area, but we believe that technology-specific regulation is premature at this time. Although the EU and the U.S. have different legal frameworks for protecting consumer privacy, we believe that enforcement of existing laws, coupled with industry self-regulation, is the best way to address consumer privacy and data security concerns related to the deployment of RFID technology.

Article 3.6: The RFID application operator should make the privacy impact assessment, or an adequate and comprehensible summary of it, publicly available through appropriate means, no later than on the date of deployment of the application.

FTC staff supports transparency with respect to companies' deployment of RFID and has encouraged companies to publicize to consumers how their information is being collected and used. However, with respect to the provision in Article 3.6 that the privacy impact assessment be made public, the staff of the FTC suggests that the EC clarify that the information to be made public should relate to the entity's privacy and information sharing practices and not to its information security measures. FTC staff believes that making public information related to data security measures might increase the possibility of making the application more vulnerable to hackers or other types of security threats. For the same reason, although FTC staff agrees that it is important to make interested stakeholders aware of the privacy practices that govern a particular application, such as in an online privacy statement, we have some concern about mandating that a company publicize identified security risks.

Article 4: Codes of Conduct

Article 4.1: Member States should encourage trade or professional associations or organizations involved in the RFID value chain to provide detailed guidance on practical implementation of RFID technology by drawing up specific codes of conduct on RFID use. Where appropriate, this work should be undertaken in collaboration with the concerned civil society organizations, such as consumer organizations or trade unions, and/or the competent authorities concerned. Codes of conduct should contain specific measures designed to ensure that signatories adhere to their principles. They should be widely disseminated with a view to informing affected individuals.

FTC staff agrees with the Commission that industry, in conjunction with other stakeholders, should be encouraged to provide guidance on practical implementations of RFID. As stated above, the FTC has long supported meaningful and effective industry self-regulation. However, the FTC does not explicitly endorse industry guidance.[10] Instead, we consult with industry about their obligations and encourage them to develop meaningful standards that will protect consumers.[11]

---

[10] This is because of potential conflicts that might arise as a matter of policy as a result of the FTC's role as the agency responsible for enforcing laws related to consumer privacy.

[11] The FTC may, however, challenge material misrepresentations to consumers regarding a company's privacy and security practices, including those set forth in self-regulatory guidelines publicly endorsed by a company.

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 its counterparts in the EC to focus on a risk-based approach to information security risk management that takes into account risks beyond the point of collection through the entire lifecycle of the data (including access controls, security of data in transmission and at rest, and secure disposal of data). FTC staff agrees with the suggestion in the Draft Recommendations that "[t]he security threats, and the corresponding security measures, should be understood as covering all components and interfaces of the RFID application." We encourage the EC to clarify that this applies to back-end databases, as well as front-end application interfaces.

Article 7: RFID use in Retail

Article 7.2: RFID application operators, where appropriate in connection with retailers, should adopt a harmonised sign to indicate the presence of tags within retail products…

The FTC generally supports efforts to promote consumer awareness and transparency in the marketplace. The FTC has long advocated a program of consumer outreach in order to empower consumers to prevent harm, rather than just responding to issues after the fact. Mechanisms such as symbols or logos can be a good way to provide information to consumers about specific products and about the choices they may have with respect to those products.

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 application processes personal data or the privacy impact assessment…shows significant likelihood of personal data being generated from the use of the application, the retailer has to follow the criteria to make the processing legitimate as laid down in directive 95/46 and to deactivate the RFID tag at the point of sale unless the consumer chooses to keep the tag operational. (b) Where a RFID application does not involve processing of personal data and where the privacy impact assessment has shown negligible risk of personal data being generated through the application, the retailer must provide an easily accessible facility to deactivate or remove the tag.

FTC staff applauds the EC's commitment to examining potential privacy and data security issues at an early stage of deployment of the technology. However, FTC staff notes that item-level tagging of consumer products is still relatively rare, and that the information stored on RFID tags in most cases does not include personal information. Rather, as noted in our 2005 RFID Workshop Report, many of the privacy and data security concerns raised by current uses of RFID technology relate to how data collected using RFID are stored and linked to back-end databases containing personal information, and whether these back-end databases are secure.

At this stage of deployment of RFID technology in retail – where item-level tagging is still relatively rare – FTC staff sees the need to gather more information about exactly how the technology will be used, including what benefits it might have for consumers in terms of convenience and product safety. In addition, we would like to have a better understanding of the potential post-sale benefits of RFID technology for consumers, such as for product recalls, before advocating a specific technological approach to protecting consumer privacy. As stated above, the FTC advocates a flexible, risk-based approach to privacy and data security. The FTC also cautions against mandating specific technological safeguards that might become obsolete or that might not be the best option for consumers under the circumstances. Similarly, with respect to RFID, we caution against mandating a specific technological approach, such as mandatory deactivation of tags, before fully understanding the range of benefits the technology might provide to consumers, as well as the range of protective measures that might be available to consumers in the future.

Article 8: Awareness raising actions

Article 8.1: Member States, in collaboration with industry and other stakeholders should take appropriate measures to inform and raise awareness among companies, in particular SMEs, on the potential benefits associated to the use of RFID technology. Specific attention should be placed on information security and privacy aspects.

As described above, the staff of the FTC believes that awareness raising actions are vitally important, particularly in the context of an emerging technology such as RFID. The FTC

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 consumer-facing RFID applications, however, the FTC believes that mandating or encouraging specific technological tools for protecting consumer privacy is premature.

The staff of the FTC looks forward to continuing to work with its EC counterparts on these and other important emerging issues to develop effective policies and practices that protect consumers and encourage responsible industry uses of RFID. Please feel free to contact Hugh G. Stevenson, Deputy Director in the FTC's Office of International Affairs, at hstevenson@ftc.gov or 202-326-3511, or Kathryn Ratté, Senior Attorney in the FTC's Bureau of Consumer Protection, at kratte@ftc.gov or 202-326-3514, if you have any questions or would like any additional information about the issues raised in this Staff Comment.