



BOARD APPROVED POLICY

**Food Marketing Institute
Policy Statement on Consumer Privacy
Adopted January 23, 2000
[Revised by FMI Board on May 1, 2004]**

We live in an era of unprecedented growth in the collection, dissemination and use of consumer data. Aggregate information derived from consumer purchases helps retailers and manufacturers better understand the needs of their customers, which, in turn, improves efficiency and lowers costs. Food retailers also have the ability to use personalized information as part of company marketing programs that benefit customers through special promotions, attractive merchandise discounts and new product offerings.

Despite these advantages, the collection and utilization of consumer data raises concern that the privacy of individual consumers could be compromised. Recognizing this concern early on, the Food Marketing Institute (FMI), a non-profit association representing more than 1,500 food retailers in the United States and around the world, developed a voluntary Policy Statement on Consumer Privacy in 1991. The policy was intended to provide guidance to members on integrating their business objectives with the privacy concerns of their customers in the rapidly expanding Information Age.

Information, in fact, is driving fundamental change in the relationship between retailers and their customers. While food retailing largely remains a mass merchandising industry, companies increasingly are able to utilize consumer purchase data to micro-market products and services to individual customers. Loyalty card or “frequent shopper” programs, which a number of retailers have implemented, offer special discounts and premium offers to customers who choose to participate. Another potential source of individualized service is the Internet, which largely is dependent upon information supplied by consumers about their product preferences, lifestyles, and other personal matters. Grocery store pharmacies offer retailers the opportunity to create targeted marketing, updates on medications and medical compliance programs (e.g., refill reminders) using prescription related data.

Emerging electronic Product Code (EPC) technology also holds the potential to improve the shopping experience of supermarket customers and to dramatically improve the efficiency of the supply chain. Retailers understand, and are sensitive to, the privacy issues arising in this new, data-rich environment. A number of companies, in fact, already have strong privacy policies in place. In the meantime, consumer privacy has become a cutting-edge issue for federal and state regulators, the news media and consumer organizations. In light of these developments, FMI re-evaluated its 1991 Consumer Privacy Policy *in 2000, and again in 2004*, and is adopting an updated version designed to reassure customers that the industry remains committed to protecting consumer privacy in a rapidly changing world.

Policy

The Food Marketing Institute and its members support the consumer's right to privacy. It is the policy of the FMI Board that it is not appropriate to sell, rent, or relinquish personally identifiable information to third party vendors, suppliers, or marketers. FMI recognizes that transaction data is a resource that retailers can use on a confidential basis to improve customer service, lower costs and create personalized merchandising and marketing programs for their shoppers who desire to participate.

Recommendation and Guidelines

The Food Marketing Institute recommends that each of its members adopt a customer privacy policy. FMI believes it is in the industry's best interest to develop a voluntary privacy standard that provides strong public assurance that the retail food industry is acting in good faith to protect the privacy of individual consumers.

The food retailing industry supports the following privacy guidelines:

□ **Notice**

Retailers should inform their customers that information about their transactions is being tabulated and stored electronically in the retailer's databases and may be used internally as part of special merchandising and promotion programs. Customers also should know that the retailer may disclose non-personally identifiable compilations of information to third parties for marketing related purposes.

□ **Choice**

Customers should be offered the opportunity to have their names removed from the retailer's database for internal marketing programs.

□ **Security**

Companies must maintain strict procedures to prevent unauthorized access, alteration, or dissemination of personalized information. Customer data, even in the aggregate, should be restricted and accessible only to those employees with a "need to know" authorization.

□ **Access**

Customers should have access (based upon written request) to any *of their own* readily available and easily retrievable purchase information stored in retailer databases.

□ **Unauthorized Access**

Unauthorized use of personally identifiable consumer information by third parties should be punishable under the law. FMI supports both federal and state legislation that would make it illegal for unauthorized third parties or individuals to access, intercept or receive an EPC signal or to disseminate information unlawfully accessed or intercepted.

Confidentiality of Prescription Drug Records

For those FMI members that operate in-store pharmacies, special consideration must be given to privacy issues related to personally identifiable medical or health information. The following additional guideline is intended for companies with pharmacies:

□ **Patient Confidentiality**

Retailers and their pharmacies affirm that personal health and medical information is – and should be – private.

- FMI supports a uniform national medical confidentiality policy that permits the interchange of personally identifiable information among health care entities for purposes of professional treatment, insurance reimbursement, or improved health care outcomes.
- The presentation of a prescription by the patient, or request for prescription refill, is considered valid approval for the pharmacy to exercise its professional responsibilities, such as drug utilization review (DUR) and evaluation (DUE).
- Pharmacies will not transfer transaction data to third parties for marketing purposes without the express consent of customers. Customers should be offered the opportunity to have their names removed from the pharmacy database for internal marketing programs.