

Farm Credit Administration

1501 Farm Credit Drive
McLean, Virginia 22102-5090
(703) 883-4000

INFORMATIONAL MEMORANDUM



July 29, 2003

To: Chairman, Board of Directors
Chief Executive Officer
Each Farm Credit System Institution

From: Roland E. Smith, Chief Examiner
Office of Examination

Subject: Recommended Elements of a Privacy Policy

The Internet serves as a source of vast amounts of personal information. Farm Credit System (System) institution Web sites may actively collect personal information through a variety of means, including registration pages, surveys, online banking, application forms, and other forms. Web sites may also use more passive means to collect personal information, such as through "cookies." A "cookie" is a file placed on the hard drive of a visitor to a Web site that allows the Web site to monitor the visitor's use of the site, usually without the visitor's knowledge.

Section 618.8300 of the Farm Credit Administration (FCA) regulations governs the handling of borrower/shareholder information, which includes any information collected from a System institution Web site. This regulation provides:

"Except as necessary in performing official duties or as authorized in the following paragraphs, no director or employee of a bank, association, or agency thereof shall disclose information of a type not ordinarily contained in published reports or press releases regarding any such banks or associations or their borrowers or members."

The Federal Trade Commission (FTC), which has been involved in addressing online privacy issues, has recognized certain core principles of fair information practices. These core principles are designed to ensure that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests. Although the FTC does not have the authority to enforce these core principles, we believe that System institutions should adhere to them when establishing a Privacy Policy. Visitors to a Web site should be provided:

- **Notice** of the institution's information practices. Visitors should be given notice of the information practices before any personal information is collected from them. Without such a notice, a visitor cannot make an informed decision as to whether and to what extent to disclose personal information.

- **Choice** with respect to the use and dissemination of information collected from or about them. Choice means giving visitors options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information, i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the visitor on a mailing list in order to market additional products or promotions, or external, such as transferring information to third parties. A visitor to a Web site may decide not to provide any personal information depending on how the Web site intends to use the information.
- **Security measures** to protect the security and integrity of any information collected. Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

Thus, to meet these core principles of fair information practices, every System institution Web site should include a Privacy Policy statement, which describes the uses of information, even if the site does not collect any information. The most effective disclosures of privacy practices are clear, prominent, and easy to understand. In general, effective disclosures are written in plain English and avoid communicating complicated information in a complex and technical way. A Privacy Policy should be posted at locations on the Web site where it will be the most meaningful. For example, if a System institution allows on-line credit applications, the Privacy Policy should be displayed at the point where personal information is collected.

Based on these core principles, we believe that at a minimum a Privacy Policy should include:

1. **Introductory Language.** Web sites are the front door for many contacts by individuals with a System institution. Having clear overview language on the privacy practices at the start of the Privacy Policy can provide a helpful introduction. Web Privacy Policies can reassure individuals that information a System institution collects about them when they visit a site will be well and appropriately handled. For example, a System institution may want to state that it limits employee access to confidential information.
2. **Description of Information Collected and Stored Automatically.** In the course of operating a Web site, certain information may be collected automatically by cookies. In some instances, System institutions may have the technical ability to collect information and later take additional steps to identify people, such as by looking up static Internet Protocol addresses that can be linked to specific individuals. A System institution Privacy Policy should make clear whether or not this type of information is collected and whether it will take steps to collect more information.
3. **Treatment of Information Collected from E-mails or Web Forms.** Many Web sites receive identifiable information from e-mails or web forms. System institutions should include a statement about how the identifiable information is treated when the individual provides it. One general and helpful comment is to say, as appropriate, that the System institution uses information included in an e-mail or Web form for the

purposes provided and that the information will be destroyed after this purpose has been fulfilled.

4. **Security, Intrusion, Detection Language.** Many Web sites use information collected on a site to detect potentially harmful intrusions and to take action once an intrusion is detected. In some situations, the policy may be not to collect personal information. In the event of authorized law enforcement investigations, however, and pursuant to any required legal process, information from Web sites and other sources may be used to help identify an individual.
5. **Weblinking.** The Privacy Policy must include a statement on Weblinking if the site links to another site. If there is Weblinking, the visitor will be subject to the other site's Privacy Policy when the visitor is at the other site. Additional FCA guidance was previously provided in the Informational Memorandums titled "Guidance for Weblinking Relationships" (September 19, 2002) and "Additional Guidance on the Risks of Weblinking" (June 4, 2003).

A Privacy Policy must be consistent with a System institution's actual practices. The institution's internal controls and policies and procedures must be consistent with the stated privacy practices in the Privacy Policy. A Privacy Policy that misrepresents an institution's practices could result in an enforcement action by the FTC for an unfair and deceptive practice and by the FCA for an unsafe and unsound practice.

The attachment to this Informational Memorandum contains some examples of Privacy Policy language adapted from United States Office of Personnel Management guidance. These examples are provided to assist in developing your Privacy Policy but may not be fully applicable to your institution's situation. System institutions should also consult their legal counsel when developing a Privacy Policy.

If you have any questions, please contact Thomas Glenn, Supervisory FCA Examiner, by telephone at (703) 883-4412 or by e-mail at glennt@fca.gov.

Attachment