



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Privacy Impact Assessment

WWW.HSR.GOV and HSR Electronic Filing System (EFS)

June 28, 2006

Introduction

The Web site www.hsr.gov will provide online public access to information and electronic forms for merging parties filing notification of proposed acquisitions for premerger review by the Federal Trade Commission and the Antitrust Division of the Department of Justice under the “Hart-Scott-Rodino” provisions of the Clayton Act § 7A, 15 U.S.C. § 18a (“HSR Act”). The HSR Electronic Filing System (“EFS”) is intended to provide a secure electronic method for merging parties to submit, and for the Agencies jointly to review, these filings, which ordinarily contain confidential business information protected by the Act. The system will also fulfill the requirements of the E-GOV Act and the Government Paperwork Elimination Act, which requires agencies, unless not practicable, to provide electronic filing, signature, disclosure and recordkeeping options for existing paperwork requirements.

Overview of System Design

The FTC, with contractor assistance, has designed and will principally manage and operate the components of the system used by the public, i.e., filing parties. The FTC will also operate the internal components of the HSR database system that already exists behind the FTC’s firewall, with modifications to accommodate EFS data. External users (i.e., filers or their designated legal representatives) will download electronic filing forms and PureEdge viewer software, from the hsr.gov Web site, which the FTC will host on its servers. The filer will use the PureEdge software to open and complete the form electronically on their own computers, “sign” the form by electronically binding it to a unique digital certificate (using public/private key technology) that the filer has obtained from a separate approved external certification authority (ECA), and then transmit the filing electronically to the Agencies in encrypted form, as described further below. Once the filing has been received by the Agencies’ own servers, the form will be decrypted, and the confidential data extracted from the form will be available to both Agencies electronically for the premerger review required by the statute.

Collection of Personally Identifiable Information

Although the forms are used to collect information from filing parties about their proposed corporate acquisitions, the EFS will collect only limited amounts of personally identifiable information incidental to the filing, as described more fully below. Nonetheless, in accordance with OMB Memorandum M-03-22 (Sept. 26, 2003), the FTC, as the agency principally responsible for the technical operation and management of the system on behalf of the reviewing Agencies, has prepared the following privacy impact assessment (“PIA”). This PIA analyzes how the information is handled to ensure that applicable legal, regulatory and policy requirements for privacy are observed; to determine the risks and effects of collecting, maintaining and disseminating any personally identifiable information in an electronic information system; and to examine and evaluate protections and alternative processes for handling the information to mitigate potential privacy risks. *See id.* at Att. A, § II.A.6.

Analysis

1. What information will be collected?

Weblog information (visitors to the Web site generally): When someone visits the hsr.gov site, it will collect only standard Web log information about that person's visit, such as the Internet Protocol ("IP") address of the computer the person is using, the browser software the person is using, his or her operating system, the date and time the person accessed the site, and, when applicable, the Internet address of the originating Web site.

Information submitted through EFS (users of the electronic filing forms): If the person downloads and submits the electronic premerger notification forms, he or she will be asked to submit the same information that they would submit on the paper version of the forms. Since these forms are designed for corporations making acquisitions subject to antitrust review by the Agencies, the forms collect information relating to businesses, not individuals. Nonetheless, as part of that process, the forms require some miscellaneous information in identifiable form, e.g.: taxpayer identification number, which could be a Social Security number of an individual in some cases; names, titles, firms, business addresses, telephone and fax numbers, and e-mail addresses of contact persons regarding the report and for purposes of receiving notice of requests by the Agencies for additional information from the filer; names of shareholders, who may be individuals in some cases; and the name, title, and, with the electronic form, the digital signature (i.e., digital certificate) of the person submitting the form, and e-mail addresses, some of which may pertain to individuals.

We note that, when persons obtain the necessary digital certificate from the external certification authority (ECA), they will need to go to a separate Web site operated by a private company (currently Verisign), which has been approved by the United States Department of Defense (DOD). The process used by the ECA to issue the required digital certificate requires individuals to supply certain personally identifiable information that is used to verify their identities before the ECA will issue an individual a certificate. The personal information that the contractor collects as part of that process is described in greater detail on the designated ECA's Web site. As this process is not under the Agencies' control and these certificates may be used for purposes other than the EFS, the issuance of those certificates is not part of this PIA. The Agencies will not receive any personally identifiable information provided to the ECA, except for the digital certificate verifying the identity of the filing individual when that person submits a filing through the HSR electronic filing system.

2. Why is the information being collected?

Weblog information: This information is collected routinely and automatically by Web sites about all visitors and is necessary for security and site management purposes. It would not be feasible to discontinue collection of this information in light of these purposes.

Information submitted through EFS: The Agencies are required to review proposed acquisitions of a certain transaction size, and the forms are necessary in order to ensure that relevant information about the transaction is consistently identified and reviewed in a timely manner. Any personally identifying information that is incidentally collected on these forms is needed for contact, payment processing, debt collection, and reporting purposes. The filings are required by the Act. Likewise, it is necessary to collect other identifying information, including taxpayer identification number required under 31 U.S.C. § 7701, in order to collect and report payments, since the collection of fees is mandated by appropriations law and funds the agency's work. Finally, the Agencies must ask the filer to attach a digital certificate to ensure the authenticity and integrity of the filing and guard against unauthorized alteration or access. In light of the highly confidential nature of these filings, which are strictly protected by the HSR Act, such a secure system is necessary. Moreover, alternatives to this signature information, such as a bare electronic signature image, could not be reasonably authenticated for legal purposes, and would be less protective of confidentiality and privacy than the digital certificate.

If it is deemed necessary for proper and effective system administration, the system may also collect and maintain email addresses from filers. The principal reason for collecting and maintaining this information would be to notify filers of any significant changes in the filing process, or for other contact purposes, in case of questions about or errors in the filing. Such notice may be necessary if, for example, we learn of vulnerabilities or other security or privacy issues with the e-filing process that may require filing parties to come back to the hsr.gov Web site to download security patches or updates for previously downloaded forms or software before attempting to submit a filing. Although the Agencies could rely simply on providing notice of such issues via the hsr.gov Web site, attempting to notify previous filers individually was determined to add a useful and appropriate additional means of notifying and protecting individuals from potentially compromising the security of their data if they failed to visit the Web site periodically for Web site, as instructed. Most e-mail addresses will likely pertain to individuals acting in their business capacity and, in any event, would be maintained in a secure manner behind the FTC firewall. Moreover, this information would be electronically deleted one year after it was collected, which tracks the one-year period of validity for the digital certificates that are required for filing, which should reduce the likelihood of maintaining outdated and inaccurate e-mail information. Such e-mail addresses are not intended to be sold or used for any marketing purposes. Thus, overall, it was determined that the potential benefit of collecting such e-mail addresses and the safeguards that will protect such information, on balance, would likely outweigh the relatively minimal privacy risk associated with the collection or maintenance of such information.

3. What are the intended uses of the information?

Weblog information: This information may be used to determine the number of visitors to the Web site, and determine if it is working properly (*e.g.*, unexplained gaps in Web site traffic). In addition, this information assists in helping to create a more useful site, and can be used for other management and security purposes (*e.g.*, to decide if greater resources are needed

to support the site, which pages are most frequently visited, whether the site is being targeted for attack by hackers, etc.).

Information submitted through EFS: As required by the Act, the principal use of this information is for the Agencies to review the proposed acquisition for compliance with the Act. Any personally identifiable information, as noted above, is collected only incidentally as part of this process, and may be used for contact, payment processing, debt collection, and reporting purposes. The digital certificate is used to verify the identity of the individual and ensure that he or she is authorized to file on behalf of the filing party. As described earlier, e-mail addresses could be collected for system administration and contact purposes.

4. With whom will the information be shared?

Weblog information: This information is not normally shared or disclosed, except as may be authorized or required by law (e.g., in response to legal process).

Information submitted through EFS: The HSR Act strictly prohibits the reviewing Agencies from sharing or publicly disclosing this information, except as may be relevant in judicial or administrative proceedings. The law also does not prohibit disclosures to either house of Congress or any duly authorized Congressional committee or subcommittee. Thus, the information will normally be shared only between the two reviewing agencies, i.e., FTC and the Antitrust Division of the Department of Justice. The personally identifiable information that is incidentally collected with the filing, may be shared with other agencies or contractors for payment processing, debt collection, and reporting purposes. The digital certificate information, to the extent that any is maintained by the system after decryption, will not normally be shared or disclosed except as authorized or required by law (e.g., in response to legal process). On occasion, the Agencies or its contractor contemplate that they may consult with GSA or its contractor if there are technical questions about the validity of a certificate or its issuance. Any information pertaining to individuals, to the extent it is retrieved from an agency system of records by their name or personal identifier, is further protected by the Privacy Act of 1974, and may be disclosed only as authorized by that Act. *See infra* Section 7 of this discussion.

5. What notice or opportunities will individuals have to consent to the collection and sharing of the information?

Weblog information: As noted earlier, it would not be feasible for security and site management reasons to discontinue the collection of this information, either for the entire site or upon request by individuals. Such an option would evade the purposes for collecting such information.

Information submitted through EFS: While the HSR Act makes premerger filings mandatory for parties proposing acquisitions that fall within the scope of the Act's filing requirements, use of the EFS is optional and voluntary. In other words, filers who do not wish to file electronically, despite the significant security controls and safeguards built into the system,

may decline to do so and continue filing by paper means. Regardless of the means of filing, the Agencies, consistent with the HSR Act, cannot legally provide filers an opportunity to limit the collection or use of the information for purposes authorized by the Act. Likewise, because filers are required to pay filing fees, the Agencies cannot provide an opportunity for filers to limit the collection or sharing of relevant information for payment processing, debt collection, or reporting purposes. In particular, we are required to collect taxpayer identifying numbers pursuant to 31 U.S.C. § 7701. It is also not feasible for the EFS to provide an option for the filer not to attach their digital certificate, as the certificate is integral to the security and authentication of the electronic filing, as explained below.

6. How will the information be secured?

Weblog information: This information will be maintained separately and securely behind the FTC's server firewalls and can be accessed only by authorized agency personnel or contractors. Moreover, the Web site itself is maintained on a secured server (https), even though the information on the Web site is all public.

Information submitted through EFS: Two methods of cryptography are used to ensure the integrity of each electronic submission. First, a digital signature binds the identity of the individual to a public/private key pair and is contained in the digital certificate issued by Verisign known as External Certificate Authority (ECA) as described earlier. This certificate offers authentication, data integrity, and technical non-repudiation. Second, during the submission process, the entire filing package is encrypted with a Verisign Class 1 encryption certificate. This filing submission process is also protected by a 128-bit secure socket layer (SSL) connection. Decryption occurs only after the package is secured behind the firewall on the FTC's internal network.

Inside the firewall, the EFS is made up of the following components: the form processing application and the submission receipt system.

The form processing application parses out the form data and distributes it to the FTC Premerger Notification Office (PNO) and DOJ Antitrust Division. The FTC copy of the parsed data is stored in a schema dedicated to the premerger notification program in a secure, designated FTC server database. The form data that is provided to DOJ are transmitted via a secure private/public RSA application. The DOJ and FTC have private, redundant T1 lines linking the two Agencies, to help ensure data security, integrity and continuity of operations.

The underlying internal Premerger submission receipt system is a secure Oracle-based client server forms and reports application that has been in production since FY97. For the user at the FTC (also available to DOJ if needed), the external EFS that filers use to submit their filings may be viewed as a built-in extension of the existing internal Oracle Forms application. This Oracle forms application can display data received electronically via EFS as well as data manually entered by FTC staff from within the application for the premerger analysis and approval process. Access to such display is passworded and limited to authorized FTC

Privacy Impact Statement – WWW.HSR.GOV and HSR Electronic Filing System

June 28, 2006

Page 6 of 8

personnel only as: (1) metadata viewed inside a client (i.e., FTC) server form, which mirrors the data that were transmitted by the outside filer using the PureEdge HSR filing form; and/or (2) through Documentum, a Web-based content management system product currently used by the FTC, which is how attachments to the electronic filing would normally be accessed and reviewed by FTC premerger staff. For any given attachment, a unique URL is used to identify it within the Premerger Oracle (FTC) client server environment, where a list of the documents is provided to the authorized user for a given premerger filing. Once the user authenticates to Documentum, a web session cookie is enabled to allow the user to access subsequent documents in that session without needing to re-enter their password. Requiring re-entry of the password for each access during a session was deemed to be unnecessarily burdensome and would potentially interfere with the timely legal review of documents, where it was possible to reduce the possible risks of an open session by having the session cookie “time out” if the user leaves the session open and unsupervised, or otherwise remains idle, for a specific period of time. By policy, users are not authorized to download data sets onto portable media, and may incorporate data from the filings into other agency documents strictly for internal review and recommendation purposes only. Data printouts on paper are likewise treated confidentially and may be disposed of only in authorized agency burn bags.

For external filers, the PureEdge software that is used to view, open and fill out the electronic forms is not itself an online application, so it is not vulnerable to the online risks that would otherwise be associated with such applications. Once the form is completed, the filer’s use of the digital certificate to “sign” such forms protects against the corruption or alteration of the data when it is transmitted over the Internet, as described above. Moreover, the external components of the filing, such as the PureEdge software, do not involve the placement of data cookies on the filer’s computer that could be used to track the individual’s usage or identity. We note that the EFS is principally designed to protect the highly sensitive nature of the filings, which are strictly protected by statute, and have much higher sensitivity than any individual identifying data that may also be incidentally collected. Accordingly, that protection is clearly sufficient to protect to any data pertaining to specific individuals or individual identifiers, and such data will ordinarily pertain only to individuals in their business rather than personal capacity, so the overall privacy risk in this system is minimal.

Internet Explorer users of the system will be required, however, to set their browsers to allow “Active X” controls in order to install an end user ECA authentication Verisign certificate. Once the ECA certificate installation is complete, the Active X security settings can be reset after the filing session so as not to use Active X, in order to prevent exposure to possible misuse or exploitation of Active X controls by other malicious, privacy-compromising programs or software that the filer may knowingly or unknowingly receive from other sources. The same is also true for an end user who uses a Netscape browser, except that instead of Active X, Javascript needs to be enabled, but may be disabled after the filing is completed to eliminate the risk that Javascript could be improperly exploited.

Finally, in accordance with OMB Memorandum M-03-22, applicable IT security requirements and procedures required by federal law and policy have been and will be followed

to ensure that information is appropriately secured. In developing this project, an appropriate risk assessment has been conducted to identify appropriate security controls to protect against risks, and those controls are implemented. Monitoring, testing, and evaluation occurs on a regular basis to ensure that controls continue to work properly and that information is safeguarded. The FTC's Chief Information Security Officer shall be the point of contact for any security questions relating to this project.

7. What are the individual's rights, if any, under the Privacy Act of 1974 or other applicable privacy laws?

Weblog information: This information is not routinely maintained or retrieved by name or other personal identifier within the meaning of the Privacy Act of 1974.

Information submitted through EFS: This information is also not routinely maintained or retrieved by the names of any individual who may be identified in filings but, rather, only by names or other data pertaining to corporate filing parties, whom the Privacy Act does not protect. Moreover, any information identifying specific individuals would ordinarily pertain to them in their business, rather than their individual, capacity, and would not be protected by the Privacy Act. Nonetheless, to the extent that the forms may collect SSNs or other information that may be retrieved and would pertain to individuals in any personal capacity for payment processing, debt collection, or reporting purposes, such information may, in such cases, be subject to the Privacy Act of 1974. *See, e.g.,* FTC System I-1 (investigational, legal and public records). Accordingly, the Web site privacy policy to be posted on hsr.gov, and a statement on the filing forms themselves, provide information that would be sufficient to satisfy the information collection notice requirements of that Act, as well as hyperlinks in the privacy policy to relevant system of records and a discussion of an individual's Privacy Act rights.

8. Other individual privacy considerations or analysis

Children's Online Privacy Protection Act (COPPA): Neither the Web site nor the EFS is subject to COPPA, since neither is directed to children under 13.

Cookies: As noted earlier, none of the external components of the filing system used by the filer, including the PureEdge software used to open and view the forms, places session or permanent cookies that could be used to track or identify the filer on the filer's computer. Session cookies are only used internally with the agency in connection the viewing of filed documents through the Documentum content management system.

Privacy Impact Statement – WWW.HSR.GOV and HSR Electronic Filing System
June 28, 2006
Page 8 of 8

Prepared for the Business Owner of the System, the Bureau of Competition, by:

/x/

Robert L. Jones, Deputy Assistant Director
Premerger Notification Office, Bureau of Competition

Review:

/x/

Alexander C. Tang, Attorney
Office of the General Counsel

/x/

Privacy Steering Committee
By: Judith Bailey, Chair

Approved:

/x/

Stephen Warren
Chief Information Officer
Federal Trade Commission