CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY
regarding the
Model Privacy Form, FTC File No. P034815

The Center for Democracy & Technology (CDT) respectfully submits these comments to the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Securities and Exchange Commission (collectively, the "Agencies") in response to the *Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*.

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies that preserve civil liberties and democratic values on the Internet. As a long-time privacy advocate, CDT has consistently sought policies and tools that give people the ability to take control of their personal information and make informed, meaningful choices about the collection, use and disclosure of personal information.

CDT commends the Agencies for conducting thorough research in their endeavor to make financial privacy notices as effective as possible at communicating vital information to consumers. CDT believes the Agencies succeeded in producing a model form that is clear and comprehensible, and we are hopeful that consumers will be able to use the notices to easily compare practices among different financial services institutions. As a current study confirms, providing consumers with accessible, readable information can cause them to make better decisions about protecting their privacy.[1] CDT views the *Interagency Proposal* as a positive step in that direction.

CDT has a handful of suggestions in response to some of the open questions raised in the model form proposal. As described in greater detail in the sections below, CDT recommends that the Agencies take the following steps:

[1] Janice Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," The 6th Workshop on the Economics of Information Society (WEIS), (Jun. 2007) http://weis2007.econinfosec.org/papers/57.pdf. The study finds that consumers who are offered accessible, understandable privacy information about online retailers are more likely to make purchases from retailers that are more privacy-protective.

1. **Add an optional "access" section to the model form** to allow financial services institutions to communicate their access and correction policies for their customers' personal information;
2. **Require clear disclosure of privacy policy changes**, so that the model form alerts consumers of any changes in an institution's privacy practices that have occurred since the last notice was issued;
3. **Research and design a Web-based form** that includes a simple Web-based opt-out mechanism;
4. **Provide downloadable model form templates** to make it easy for financial institutions to create their own privacy notices based on the model;
5. **Omit the "Account number" field from the opt-out section** to reduce the risk of fraud related to the use of the opt-out feature; and
6. **Monitor the uptake of the model form** to determine the level of adoption among financial institutions, whether steps may be needed to encourage uptake, and whether consumers can easily compare notices from different institutions.

1. Optional Access and Correction Section

The *Interagency Proposal* seeks comment on whether the model form provides the opportunity for financial institutions to accurately and sufficiently disclose their privacy practices.[2] CDT believes there is a set of practices – those involving access and correction of personal information – that may warrant an additional section on the model form.

Many financial institutions maintain policies that allow their customers to request access to the personal information that is held about them and to suggest corrections if they discover errors. Some institutions are required to do so by the Fair Credit Reporting Act, while others may choose to do so voluntarily. CDT believes that the model privacy form is an appropriate and convenient vehicle for financial institutions to communicate access and correction procedures to their customers. As such, CDT recommends that the Agencies include an optional section in the model form where institutions wishing to do so can describe how consumers may access and/or correct their personal information.

CDT would suggest specifying that an access and correction box may be included on page 3 of the form, immediately following and with a similar format to the "If you want to limit our sharing" box that the Agencies have suggested on the top of that page. The access and correction box would briefly inform customers about the existence of an access/correction process and how to go about launching it. Of course, this is just one example of how the optional access and correction information could be incorporated into the model form, and the Agencies should conduct consumer testing during the second research phase to determine the most effective way to express this access information.

[2] *See Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*, FTC File No. P034815, (Mar. 2007) at 31, question #2.

2. Disclosure of Changes to Privacy Policy

The Agencies are requesting input on "whether financial institutions should be required to alert consumers to changes in an institution's privacy practices as part of the proposed model form."[3] CDT's answer is a resounding yes. Consumers interact with multiple institutions and hence can receive many notices, making it unlikely that they will carefully review every policy every year. Particularly since consumers' relationships with their financial institutions can last for many years, clear disclosure of what has changed may be some of the most valuable information they will gain from an annual privacy notice. Providing a standard, concise way for institutions to communicate key changes will allow consumers to more easily make decisions about their privacy on a consistent basis.

The information about privacy policy changes could be communicated in several ways. For example, the Agencies could add a column to each of the boxes on page 1 and the "Sharing practices" box on page 2 with a heading such as "Changed since last notice?" The entries in the column would either describe the updates that have taken place for that particular row item or would be filled in with "No" if no updates had taken place. Alternatively, there could be a separate box or section on page 1 or page 2 that describes all of the privacy updates in one location. There may be other ways to communicate this information as well – CDT suggests that the Agencies research and test how best to express privacy practices changes and choose the implementation that will likely be most effective.

3. Web-Based Model Form

The *Interagency Proposal* seeks comment on whether the Agencies should create a Web-based model form and what design and technical considerations should be made in the development of such a form.[4] CDT strongly encourages the Agencies to develop a Web-based version of the model notice.

A recent study has shown that nearly half of all Internet users engage in online banking.[5] Online delivery of financial privacy notices would be a sensible, efficient way to inform consumers who are already accustomed to interfacing with financial institutions online. A Web-based notice can also provide a simple means for consumers to opt out of information sharing at the click of a mouse.

Just as the Agencies conducted extensive research to determine the best format for the paper notice, so too should they investigate how the notice information may be best presented on the Web. While the three-page layout works well in paper form, the

---

[3] *See Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*, FTC File No. P034815, (Mar. 2007) at 31, question #5.

[4] *See Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*, FTC File No. P034815, (Mar. 2007) at 32, question #4.

[5] Susannah Fox and Jean Beier, "Online Banking 2006: Surfing to the Bank," Pew Internet & American Life Project, (June 2006) http://www.pewinternet.org/pdfs/PIP_Online_Banking_2006.pdf.

Agencies should determine whether multiple Web pages or a single page would be most easily read online.

The Agencies should also consider providing the ability for institutions to link between different pieces of information within the notice, such as between terms (for example, "affiliates") and the definitions of what those terms mean. The answers to the "Can you limit this sharing?" question in the disclosure table on the first page of the form should link to the opt-out choices where appropriate. The Agencies might also consider making the references to "federal law" into links to Web sites hosting the text of the relevant laws where practical.

CDT suggests that the Agencies use a secure HTML form for the opt-out section, allowing consumers to submit their opt-out choices using encrypted communications over the Internet. This would give consumers the convenience of being able to opt out online at the time of their viewing of the notice. The Agencies should test the opt-out form to ensure that consumers can understand it and complete it effectively.

4. Downloadable Model Form Templates

The Agencies are seeking input on whether they should develop and make available on their Web sites "fillable" model form templates that enable institutions to easily download and create notices by filling in appropriate fields.[6] CDT encourages the Agencies to take this step, as it will simplify the process of adoption, particularly for smaller institutions. It will also likely prompt more institutions to adopt the model form than if each institution had to develop its own paper form. The more institutions using the model form, the more effective it will be as a tool for informing consumers and providing them with a basis for comparison.

Based on the inclusion of so many different example notices in the *Interagency Proposal*, it may well be that the Agencies already possess templates which are nearly in a suitable format. The benefits of providing easy-to-use downloadable templates are worth the small amount of effort that remains to make such templates available.

5. "Account Number" Field in Opt-Out Section

The Agencies are requesting comment on the necessity for consumers to provide their account number, Social Security number, or other identification number in order to opt out of an institution's information-sharing policy, or whether a consumer's name, address, and (perhaps) truncated account number would be sufficient to complete the opt-out.[7]

It is unclear to CDT that any information beyond name and address is necessary for the purposes of opting out. These two items should provide enough information for

---

[6] *See Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*, FTC File No. P034815, (Mar. 2007) at 32, question #5.

[7] *See Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*, FTC File No. P034815, (Mar. 2007) at 33, question #7.

institutions to identify the individual requesting the opt-out. Thus, CDT recommends that the Agencies remove the "Account number" field from the opt-out section.

If financial institutions feel that they absolutely need another identifier of some sort, a truncated account number is a much better choice than either full account or Social Security number. The Agencies could change the "Account number" tag to read, "[First or last 4] digits of account number," allowing the institution to choose whether the truncated portion comes from the beginning or the end of the account number.

The potential privacy risks of requiring consumers to divulge account or Social Security numbers increases dramatically in the online context, particularly due to the prevalence of "phishing" attacks. Financial institutions making use of an online privacy notice may decide to alert their users to the presence of the notice via email. If such an email contains a link to an opt-out page that requires the customer to input an account or Social Security number, that email can be easily reproduced by fraudsters who then trick consumers into divulging their personal information on a fake site that resembles the real opt-out site. Most financial institutions are already grappling with phishing issues, and it would be a mistake to compound this problem by requiring highly sensitive personal information in an online opt-out. Thus, CDT strongly discourages the Agencies from including an account number field of any kind in its Web-based model form.

6. Monitoring Model Form Uptake

The *Interagency Proposal* seeks comment on the extent to which financial institutions are likely to use the proposed model form.[8] While CDT cannot speak directly to whether institutions will make use of the form, it is our strong desire to see its wide adoption.

CDT believes that one of the main benefits of using a standard notice will be to enable consumers to more easily compare the privacy practices of different financial institutions. It is currently difficult for consumers to sort out the differences between institutions' policies, because each institution writes its notices with a different format, ordering, and lexicon. Increased comparability depends on wide acceptance and use of a common standard.

We recommend that, going forward, the Agencies continue to monitor the extent to which institutions are using the form and whether consumers can easily compare different institutions' notices. The Agencies should issue a public report of their findings, and they should consider taking steps to encourage uptake if they find that few institutions are using the model notice.

[8] *See Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act*, FTC File No. P034815, (Mar. 2007) at 32, section C, question #1.

* * *

CDT applauds the Agencies for creating a model notice that is concise and easy to understand. We appreciate the opportunity to offer these additional suggestions on the *Interagency Proposal*, and we look forward to what we hope will be widespread adoption of a standard notice that will prove informative and useful to consumers.

Ari Schwartz
David Sohn
Alissa Cooper
Center for Democracy & Technology
1634 Eye St. NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800