DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Working Party on Information Security and Privacy

MAKING PRIVACY NOTICES SIMPLE:
AN OECD REPORT AND RECOMMENDATIONS

ANNEXES
ANNEX A

Extract from the OECD Privacy Statement Generator

http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html

HOW TO DEVELOP A PRIVACY POLICY

STEP 1. To ensure that you answer the questions contained in the Generator accurately, you need to know what your personal data practices are. Therefore, before completing the questionnaire, it is essential to carry out an extensive internal review of your current personal data practices. For example:

- Do you collect personal data?
- What kinds of personal data do you collect?
- How are they collected? From individuals, from third parties, from public bodies or authorities? Are individuals aware that their personal data are being collected?
- Who in your organisation is responsible for deciding what personal data are collected and how?
- Why do you collect personal data?
- How are they used?
- Who controls personal data once they are collected?
- Are personal data disclosed to third parties, and if so, why?
- How and where are they stored?
- Do you have standards, guidelines and regulations which apply to your collection and use of personal data?
- Do you allow visitors access to the personal data you have about them?
- What happens if a visitor has a query about their personal data? What if they are not satisfied with how you deal with their query?

Further guidance on carrying out an internal review can be found on the Web sites of SIIA, USCIB, or CSA Model Code CAN/CSA-Q830.

You may also wish to consult:

www.jipdec.or.jp/security/privacy/index-e.html
www.research.att.com/projects/p3p/propgen
www.the-dma.org
www.truste.org/wizard

STEP 2. Once you have reviewed your current personal data practices:

- You should review laws or (self) regulatory schemes which may apply to your collection and use of personal data. Governmental agencies, non-governmental organisations or private bodies may provide you with help in this respect.

It is recommended that you review your current practices against such regulations and amend them where necessary to ensure compliance.
USING THE GENERATOR TO CREATE A PRIVACY POLICY STATEMENT

STEP 3. Once you have determined your current personal data practices and reviewed those practices against relevant regulatory requirements, you are in a position to complete the Generator questions. The Help Section provides explanations of terms used, guidance on what is consistent with the OECD Privacy Guidelines, and, where appropriate, additional information on other national, regional or international instruments. It is important to read the technical notes before answering the questions.

After you have completed the questionnaire as accurately as possible, a draft privacy policy statement is automatically generated. It proposes pre-formatted sentences based on your answers/choices.

ASSESSING THE DRAFT PRIVACY POLICY STATEMENT

STEP 4. Next, you should make sure:

- That the draft privacy statement accurately reflects your organisation’s personal data practices.
- That the draft privacy statement complies with applicable national, regional and international laws or (self) regulatory schemes.
- That errors are corrected and that the privacy statement reads smoothly.

PLACING YOUR PRIVACY POLICY STATEMENT ON YOUR WEB SITE

STEP 5. Once you are satisfied that your privacy policy statement accurately reflects your personal data practices and complies with applicable regulations, you need to consider how to make your statement publicly available. Regulations to which you may be subject may require a specific location for such a statement, such as your homepage, or at the point(s) where personal data are collected. In the absence of specific regulatory requirements, you may wish to consider creating a link between your homepage and your privacy statement, or between pages where you collect personal data and your privacy statement. The OECD Privacy Guidelines recommend that individuals should be able to gain access to information about personal data practices without unreasonable effort as to time, knowledge and expense. You may also wish to create links to relevant Web sites to make visitors aware of any relevant regulations.

REMEMBER: Once your privacy statement is publicly posted, you may be legally liable if you fail to abide by your privacy policy statement or if that statement does not comply with local laws.

By following the above steps, you can help ensure that your policy statement will not misrepresent your privacy practices or fail to comply with applicable regulations.
ANNEX B

Executive Summary the “Research Report on Fair Processing Notifications: Current Effectiveness and Opportunities for Improvement”, United Kingdom
Research Report
Fair Processing Notifications: Current Effectiveness and Opportunities for Improvement

Version 1.1
March 11, 2005

Contact: Dermot Browne
Corporate Solutions Consulting (UK) Limited
84-88 Pinner Road
Harrow
Middlesex
HA1 4HZ

Tel: 020 8427 7795
Fax: 020 8427 7801

Email: Corporate_Solutions@consult-me.co.uk
Internet: www.consult-me.co.uk
# Table of Contents

1 Executive Summary ................................................................. 3  
1.1 Results Summary ................................................................... 4  
2 Introduction .............................................................................. 9  
3 Research Design ....................................................................... 10  
3.1 Introduction ........................................................................... 10  
3.2 Objectives ............................................................................. 10  
3.3 Phases .................................................................................. 10  
3.4 Data Controller Survey ......................................................... 10  
3.5 Research Alternative Notification Formats ................................. 11  
3.5.1 Overall Design ................................................................... 11  
3.5.2 Procedure .......................................................................... 11  
3.5.3 Administrator’s Script ....................................................... 13  
3.5.4 Presentation Order ......................................................... 13  
3.5.5 Participants ....................................................................... 14  
3.5.6 Age Distribution .............................................................. 14  
3.5.7 Gender Distribution ......................................................... 15  
3.5.8 Social Groupings – Overall .............................................. 17  
3.5.9 Social Groupings – Regional ............................................ 17  
3.5.10 Test Materials – Credit Card Applications ........................ 17  
3.6 Stakeholder Review ............................................................... 19  
4 Results and Analysis .................................................................. 20  
4.1 Introduction ........................................................................... 20  
4.2 Approach .............................................................................. 20  
4.3 Comparative Study Questions ............................................... 21  
4.3.1 Hard copy ................................................................. 22  
4.3.2 Internet ....................................................................... 27  
4.3.3 Telephone .................................................................... 32  
4.3.4 Learning Effects Across Test Tasks .................................. 37  
4.4 Comparing Media ................................................................. 39  
4.4.1 Effectiveness ................................................................. 39  
4.5 Comparing Formats .............................................................. 40  
4.5.1 Effectiveness ................................................................. 40  
4.6 Stakeholder Comments ......................................................... 41  
4.6.1 General Remarks ........................................................... 41  
4.6.2 Attention ...................................................................... 41  
4.6.3 Understanding ............................................................... 41  
4.6.4 Memorability ................................................................. 42  
4.6.5 Awareness .................................................................... 42  
4.7 Experience, Attitudes and Expectations .................................. 43  
4.7.1 Experience with Financial Products ................................. 44  
4.7.2 Experience of Internet/Telephone Applications for Financial Products .................................................. 45  
4.7.3 Concern Regarding Small Print ....................................... 46  
4.7.4 Concern Regarding How Personal Information is Handled 46  
4.8 Post-Task Questions ............................................................. 47  
4.8.1 Learning Impact of the Study ........................................... 47  
4.8.2 Interest in Improved FPN Presentation............................ 48  
4.8.3 Essential Information Required from Institutions .............. 50  
4.9 Results Summary ................................................................. 51
1 Executive Summary

This study examined the effectiveness of Fair Processing Notifications (FPNs) across three media: hard copy, internet and telephone. The study considered FPNs in the financial sector exclusively. The objectives of the study were:

- To establish which attributes of FPNs (across all three media) are key in making them understandable to recipients;
- To establish which features of FPNs data controllers need to consider to ensure that their FPNs are effective for users at the same time as being Data Protection Act (DPA) compliant;
- To provide guidance for data controlling organisations to produce effective FPNs.

The study comprised 5 phases, the 3 principal research phases being:

- **Data Controller Survey**: survey of Financial Sector data controllers to understand their requirements for and current difficulties with FPNs;
- **Research Alternative Notification Formats**: comparative evaluation of the merits and problems associated with notifications presented in different formats, covering hard copy, internet and telephone-based FPNs;
- **Stakeholder Review**: consultation process to ascertain the practicality of changes to notifications as suggested by the research findings.

The Data Controller Survey found that despite a diversity of processes in the design and production of FPNs, there were some common themes, including:

- The complexity of the process of designing FPNs, with customers, commercial and compliance issues all needing to be balanced;
- The difficulty of getting the marketing opt-out process right;
- The effort required to produce FPN variations;
- The desire for guidance/guidelines for FPN design.

The Notification Formats study found that:

- 58.3% of participants say they ‘care’ about the small print;
- 59.8% say they ‘care’ about what happens to their personal information;
- 58.4% misunderstand what the DPA is about in relation to financial products;
- Most people have little detailed knowledge of what happens to their personal information;
- Most people learn little from FPNs irrespective of the way they are presented;
- Most people pay scant attention to FPNs;
- 71.8% would pay more attention to better designed FPNs;
- Most peoples’ behaviour is at odds with their claim to ‘care’, and most people justify the contradiction between ‘caring’ and a lack of real attention in terms of a trade-off between the perceived risk and the level of effort required.
The Stakeholder Review found that:

- Stakeholders are willing to engage in efforts to improve FPN effectiveness;
- Generally, the preliminary recommendations from the comparative study met with approval; however there are practical issues such as space for hard copy FPNs which have to be considered;
- Recommendations which imply a change to place more responsibility on data subjects are of interest to stakeholders, but may take time to implement and require the agreement of the Information Commissioner;
- Recommendations outside of FPN presentation, for example awareness programs, are of interest but are long term and require the co-operation of the Information Commissioner, industry and educational establishments.

Opportunities for improvement to FPNs can be found in:

- The design and presentation of FPNs;
- The management of FPNs to generate greater consistency of language and structure across the financial sector;
- Improving awareness of the importance of personal information, leading to changes in behaviour where FPNs are encountered.

Within these areas short, medium and long-term actions can be identified which together form an integrated strategy for improving the effectiveness of FPNs.

1.1 Results Summary

This section summarises the results in terms of the main questions for the research:

**Are FPNs effective?**

No. This study suggests that most people ignore FPNs when presented in hard copy or on the internet (they have little choice but to pay some attention over the telephone). When they do pay attention to FPNs, the study findings suggest that the messages contained in the FPNs are not assimilated – people report very little of the FPN content. With most people missing the FPNs or intentionally ignoring them, and with those that do pay some attention to FPNs unable to report much of the content, FPNs are not doing the task for which they were intended.
Why is FPN effectiveness so poor?

There are a number of reasons for poor FPN effectiveness. Many concern the design of the FPNs themselves, but the attitudes of data subjects are also important:

- Data subjects do not pay attention because they perceive the risk as low;
- Data subjects do not pay attention because they think it is ‘too late’ or ‘doesn’t make any difference if I know about it or not’;
- Data subjects do not pay attention because they are focused on the application itself;
- Data subjects think FPNs are about marketing and junk mail, and they are confident that they’ve done all they need to when they tick the ‘no marketing’ box on an application form;
- Data subjects have filled out forms and made applications before, and believe this is just more legal jargon which they will not be able to understand even if they do read it;
- Data subjects do not pay attention because they trust the financial institution they are applying to, and the Data Protection Act, to make sure everything is ‘above board’. In this research the use of a fictitious bank suggests that trust of the organisation cannot have been influencing the observed behaviour. However assumptions about the Data Protection Act may still have had an effect;
- There is a belief that the onus is not on them to protect their data, it is the institutions’ job.

When they do pay attention, data subjects often fail to read FPNs completely and do not report much afterwards because:

- FPNs are too long and repetitive;
- FPNs contain financial and legal jargon;
- Data subjects are not engaged by the FPN – for example the FPN is presented as a text in hard copy which does not require any involvement from them;
- On the internet, insufficient effort is made to use the design space offered by the technology to highlight key FPN points. In fact, websites appear to be designed to get applicants through the pages as quickly as possible, with a minimum of effort to bring FPNs to applicants’ attention;
- They read the FPN but do not perceive it as relevant, or representing a significant risk to them;
- The structure of the FPN is unclear, so it is difficult to read the main points quickly or selectively;
- There is little use of mnemonics, structured text or text cues to facilitate the memorability of the FPN material.
Is one medium more effective than another?
Yes. Telephone appears to be a better medium for presenting FPN information than either hard copy or the internet. People have to attend on the telephone in a way that they do not with the other media. The main attribute seems to be that if you believe that you might be asked a question at any moment, then you will pay attention; additionally, telephone applicants cannot skip ahead to another part of the application – the delivery is sequential. Of the three media, internet was notable for the ease with which people were able to scroll through screens. However the down side to this is that people can scroll quickly past material they need to read, such as the FPN. With hard copy, the difficulty appeared to be in identifying the material amongst the volume of paperwork.

Which formats work best, and which are preferred? Should FPNs be designed for what works ‘best’ or what is preferred?
Hard copy – Condensed works best, Condensed is preferred.
Internet – Plain works best, Layered is preferred;
Telephone – Condensed works best, Layered is preferred;
In all cases the level of effectiveness was low, and in several cases there was only a marginal difference between the best and worst performers. In designing FPNs it would seem best to take the preferred formats and make them work better than they do currently.

Is it the data subjects’ fault? Would they still not read the FPNs or remember them even if a lot of effort was spent improving them?
No, it is not the data subjects’ fault, and Yes, a majority report that they would pay more attention to the FPNs if the FPNs were more accessible (both in terms of finding them in the application material and in terms of their content). It is entirely understandable that data subjects approach the application task in ways that make sense to them but which may mean that the FPN assumes a lower priority than might be wished for. It is also entirely reasonable for data subjects to expect important material to be presented in a way that reflects its importance. A number of participants in the study noted that a lot more effort appeared to have gone into making features of the product prominent than had gone into making features of the handling of their information prominent.

Does this data generalise to other industry sectors?
This research was conducted in relation to financial sector FPNs. It is possible that the relationship between an applicant for a financial product and a financial sector data controller differs from the relationship between other consumers and their associated data controllers. However, it is likely that the findings from this research can be applied more extensively. Any such generalisation should, however, be treated with caution without evidence from the specific context.
What makes an FPN ‘good’?

The main requirement of an FPN is that it should be read, understood and remembered (in addition to containing the information required to make it legally compliant). A good FPN therefore:

- Stands out from the surrounding material (in all three media);
- Makes a very clear statement of what it is about in a title or heading, and preferably does this in a way that attracts the attention of the largest range of people. For example it makes an impact by using attention grabbing words in the title like ‘risk’ or ‘your protection’. Data subjects have to be given a reason to pay attention to an FPN;
- Is clearly distinguishable from material on marketing (reasonable steps should be taken to make it clear that the FPN, and the Data Protection Act in the financial sector context, is not about preventing junk mail);
- Requires action; people pay attention to anything in an application that requires them to do something (answer a question, tick a box, sign acceptance);
- Uses the available techniques (e.g. layering in internet and telephone forms) of easily understood writing;
- Is involving, for example by requiring data subjects to tick a box when they have read a sub-paragraph in hard copy, or requiring them to respond to a question in a telephone script;
- Uses short sentences, active voice, bullet points, and any available space;
- Is short, but not so short that data subjects will feel that information has been left out (it must at the very least contain information about credit reference checks, fraud prevention agencies, financial associates, and what happens to personal information (how long is it held for and who has access to it));
- Is not in so small a font size that it will be difficult for people to read;
- Uses mnemonics or ‘catch phrases’ consistently to get the FPN message across to readers/listeners;
- On the telephone, the script requires the adviser to announce the FPN is about to be read, and then checks that it has been listened to and (at each main point) understood;
- Is consistent in terminology and content with other FPNs from the particular organisation and as far as possible uses expressions common to the industry.

Note that the best way to promote and deliver FPN effectiveness is to specify the required performance levels in advance and to design and test to those levels. If an organisation specifies who will read its FPNs (age, educational level, experience with financial institutions), and also specifies levels of attention to, understanding and recall of FPNs, it will be able to improve the effectiveness of its FPNs.
ANNEX C

Evolution of a Prototype Financial Privacy Notice

A Report on the Form Development Project

February 28, 2006
Executive Summary

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), requires financial institutions to provide their customers with initial and annual notices of their privacy policies and practices. The notices must be clear, conspicuous, and accurate statements of the company’s privacy practices, and provide a means for consumers to opt out of certain information sharing when they have the right. Soon after the GLBA went into effect in 2001, researchers reported that the privacy notices were too lengthy, dense in content, and contained complex language; they found that most consumers neither read nor understand privacy notices.

In response to these findings, six of the federal agencies1 that enforce the GLBA initiated a project to explore the development of paper-based, alternative financial privacy notices—or components of notices—that are easier for consumers to understand and use. In September 2004, the six agencies selected Kleimann Communication Group (Kleimann) for this project entitled the Form Development Project.

Our report presents the research-based rationale for a “prototype” privacy notice iteratively designed over the course of the Form Development Project. The report discusses the methodology used for our qualitative research; presents our findings and analysis from eight test sites; describes the evolution of the prototype through a 16-month iterative process; and outlines key themes that contribute to the success of the project and to the clarity and usability of the prototype.

This report completes phase one of the Agencies’ two-part research project. Phase two, a quantitative study to be planned and contracted separately by the Agencies, will assess the prototype.

---

1 The six federal agencies are: Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, and the Securities and Exchange Commission.
The Project Objective

The project objective was to explore the reasons why consumers don’t read and understand privacy notices and to use this research to develop paper-based, alternative privacy notices—or components of notices—that consumers can understand and use. We used a rigorous, research-based design model to gather data and make revisions after each iteration based on consumer input. This process of designing and revising allowed us to continually modify general and specific features of the prototype, such as content, presentation, and wording. The process also allowed us to understand barriers to consumer comprehension and ultimately arrive at a prototype that met the project goals of comprehension, comparability, and compliance.

The Project Goals

The project had three goals:

- **Comprehension.** The prototype must enable consumers to understand the basic concepts behind the privacy notices and understand what to do with the notices. It must be clear and conspicuous as a whole and readily accessible in its parts.

- **Comparison.** The prototype must allow consumers to compare information sharing practices across financial institutions and to identify the differences in sharing practices.

- **Compliance.** The content and design of the alternative privacy notices must include the elements required by the GLBA and the affiliate marketing provision of the Fair and Accurate Credit Transactions Act.

Design Considerations

Within the design, we worked with several considerations and constraints:

- **Neutral and Objective.** The prototype needed to inform consumers about privacy laws and financial institutions’ sharing practices in a factual and neutral way. The language could and should not direct a consumer to make any particular decision. Through the course of designing and testing, we stayed away from using inflammatory or potentially provocative words as a means of attracting attention.

- **Format and Design.** The prototype must be paper-based rather than Web-based. To focus on the research goals of comprehension, comparability, and compliance and minimize testing variables, we tested only in black and white, on 8½” x 11” paper, and with a large, readable font.
Methodology

We used a varied, qualitative research-based design process to accomplish the project objective and goals. The financial privacy notice prototype evolved in content and design based on an iterative process of consumer research, rigorous data collection, thorough analysis, and the expertise of the information designers and legal experts.

Qualitative research uses small numbers of participants to explore in a realistic manner how and why consumers understand and make sense of a document. For the Form Development Project, we used four qualitative methods—focus groups, preference testing, pretest, and diagnostic usability testing—to iteratively develop and refine the prototype according to the goals of comprehension, comparability, and compliance.

Testing

We tested a total of 66 participants over eight test rounds in various locations based on the U.S. census regions and divisions. The testing was conducted over 12 months, as follows:

- Two focus groups with 10 participants in each, 20 participants total (Baltimore, MD)
- Preference testing with 7 participants (Washington, DC)
- Pretest with 4 participants (Baltimore, MD)
- Diagnostic usability testing with 35 participants in five sites (San Francisco, CA; Richmond, VA; Austin, TX; Boston, MA; and St. Louis, MO)

---

2 Focus groups and preference testing provide baseline information on consumers’ impressions, attitudes, likes and dislikes about the subject matter and the initial documents. Focus groups tell the researcher what a group of consumers thinks about privacy notices and what they see as barriers to understanding them, but they do not tell the researcher what a consumer will actually do with a notice. Preference testing uses in-depth one-on-one interviews that explore consumers’ preferences for certain vocabulary, headings, notice components, and ordering of the information. This testing informs the initial document designs. Conducting a pretest allows for a dry run of the diagnostic usability test, and validates the methodology by testing the moderator’s guide and test design. Diagnostic usability testing looks at how the individual participant actually works with a document and elicits his or her immediate reaction to the information content and design to target and diagnose problems. This testing approach allows for more in-depth probing of consumers’ attitudes toward the document and, because it is an iterative process, also allows for continual adjustment to the notice content and design with successive test rounds.
Research and Design

Each test session was carefully planned and structured to meet our research goals of comprehension, comparison, and compliance. The following five questions helped guide the development of the prototype content and design. How do we:

1. attract consumers’ attention to the notice using only objective and factual language;
2. decide what information to include;
3. ensure that consumers can understand about the sharing of their personal information;
4. ensure that consumers can compare sharing practices across financial institutions; and
5. enable consumers to understand how to opt out.

Prototype Evolution

As with most design development projects, one key challenge was how to select and organize the content of the notice to address these goals and questions. We used the information and elements required by the law, organizing them in different ways throughout the process to arrive at a final organization of the content that worked.

We developed and tested a variety of designs, ultimately structuring the disclosure of information sharing practices in a table format. We learned that we needed to include an educational component in the notice as consumers had no prior understanding of information sharing practices. To do this, we identified the key information that would draw the reader into the notice and provide sufficient information to enable understanding of the disclosure table. Supplemental information, such as definitions and additional information required by the GLBA, was provided on page 2 of the prototype. Testing showed that consumers could work with page 1 alone, although they appreciated the supplemental information on page 2 for further clarification. We also experimented with a prose design of the disclosure information, but the table design worked far better in helping consumers easily access, understand, and compare sharing practices.

The Prototype Notice

The prototype\(^3\) has four key components—the title, the frame (key and secondary), the disclosure table, and the opt-out form—that contribute in multiple ways to its effectiveness.

---

\(^3\) The prototype is intended to be used by any financial institution, but for convenience, we used fictional bank names for the notices.
The Title
The title helps consumers understand that the notice is from their bank and that their personal information is currently being collected and used by their bank.

The Frame
The frame is at the heart of ensuring comprehension because it provides basic information about financial sharing practices as a context for consumers to understand the details of their particular bank’s sharing practices. The key frame on page 1 provides a context for the consumer and gives key details. The secondary frame on page 2 also includes a series of frequently asked questions, more required information, and more detailed definitions of terms on page 1. The frame is necessary for understanding the disclosure.

The Disclosure Table
The disclosure table is at the heart of the prototype. It not only shows what the individual financial institution is sharing, but also includes seven basic reasons any financial institution can share information. The disclosure table, therefore, enables consumers to understand the details of their financial institution’s sharing practices in the context of how other financial institutions can share. It is critical for comprehension and comparability.

The Opt-out Form
The opt-out form identifies how a particular financial institution allows consumers to limit a particular type of sharing.
# Facts

**What does Neptune Bank do with your personal information?**

**Why?**

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

**What?**

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social security number and income
- Account balances and payment history
- Credit history and credit scores

When you close your account, we continue to share information about you according to our policies.

**How?**

All financial companies need to share customers' personal information to run their everyday business—to process transactions, maintain customer accounts, and report to credit bureaus. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Neptune Bank chooses to share; and whether you can limit this sharing.

## Reasons we can share your personal information

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does Neptune Bank share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For our everyday business purposes— to process your transactions, maintain your account, and report to credit bureaus</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our marketing purposes—to offer our products and services to you</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For joint marketing with other financial companies</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes— information about your transactions and experiences</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes— information about your creditworthiness</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
<tr>
<td>For our affiliates to market to you</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
<tr>
<td>For nonaffiliates to market to you</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
</tbody>
</table>

**Contact Us**

Call 1-800-878-9698 or go to www.neptunebank.com/privacy

---

**Title**

Draws consumers into the notice, helping them understand that the information in the prototype is from their own financial institution and that their personal information is being collected and used by the financial institution.
### Facts

**What does Neptune Bank do with your personal information?**

**Why?**

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

**What?**

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social security number and income
- Account balances and payment history
- Credit history and credit scores

When you close your account, we continue to share information about you according to our policies.

**How?**

All financial companies need to share customers' personal information to run their everyday business—to process transactions, maintain customer accounts, and report to credit bureaus. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Neptune Bank chooses to share; and whether you can limit this sharing.

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does Neptune Bank share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For our everyday business purposes—to process transactions, maintain your account, and report to credit bureaus.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our marketing purposes—to offer our products and services to you.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For joint marketing with other financial companies.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes—information about your transactions and experiences.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes—information about your creditworthiness.</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
<tr>
<td>For our affiliates to market to you.</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
<tr>
<td>For nonaffiliates to market to you.</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
</tbody>
</table>

**Contact Us**

Call 1-800-898-9698 or go to www.neptunebank.com/privacy

---

**Key Frame**

Provides a context for the consumer and gives key details about personal information, information sharing practices, and the laws relating to these practices. It is the heart of ensuring comprehension.
WHY?
Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires
us to tell you how we collect, share, and protect your personal information. Please
read this notice carefully to understand what we do.

WHAT?
The types of personal information we collect and share depend on the product or
service you have with us. This information can include:
• social security number and income
• account balances and payment history
• credit history and credit scores
When you close your account, we continue to share information about you according
to our policies.

HOW?
All financial companies need to share customers’ personal information to run their
everyday business—to process transactions, maintain customer accounts, and report
to credit bureaus. In the section below, we list the reasons financial companies can
share their customers’ personal information; the reasons Neptune Bank chooses to
share; and whether you can limit this sharing.

<table>
<thead>
<tr>
<th>Reasons we can share your personal information</th>
<th>Does Neptune Bank share?</th>
<th>Can you limit this sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For our everyday business purposes—to process your transactions, maintain your account, and report to credit bureaus</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our marketing purposes—to offer our products and services to you</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For joint marketing with other financial companies</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates’ everyday business purposes—information about your transactions and experiences</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates’ everyday business purposes—information about your creditworthiness</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
<tr>
<td>For our affiliates to market to you</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
<tr>
<td>For nonaffiliates to market to you</td>
<td>Yes</td>
<td>Yes (Check your choices, p.3)</td>
</tr>
</tbody>
</table>

Contact Us
Call 1-800-898-9698 or go to www.neptunebank.com/privacy

Disclosure Table
Shows seven basic reasons a financial institution can share, indicates how this bank
shares, and identifies whether the consumer can or cannot opt out. Because the
disclosure table shows both what any institution can do and what an individual
institution does, it allows consumers to compare across institutions.
# What Does Neptune Bank Do With Your Personal Information?

## Sharing Practices

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How often does Neptune Bank notify me about their practices?</td>
<td>We must notify you about our sharing practices when you open an account and each year while you are a customer.</td>
</tr>
<tr>
<td>How does Neptune Bank protect my personal information?</td>
<td>To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.</td>
</tr>
<tr>
<td>How does Neptune Bank collect my personal information?</td>
<td>We collect your personal information, for example, when you • open an account or deposit money  • pay your bills or apply for a loan  • use your credit or debit card  We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.</td>
</tr>
<tr>
<td>Why can’t I limit all sharing?</td>
<td>Federal law gives you the right to limit sharing only for • affiliates’ everyday business purposes—information about your creditworthiness  • affiliates to market to you  • nonaffiliates to market to you  State laws and individual companies may give you additional rights to limit sharing.</td>
</tr>
</tbody>
</table>

## Definitions

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyday business purposes</td>
<td>The actions necessary by financial companies to run their business and manage customer accounts, such as • processing transactions, mailing, and auditing services  • providing information to credit bureaus  • responding to court orders and legal investigations</td>
</tr>
<tr>
<td>Affiliates</td>
<td>Companies related by common ownership or control. They can be financial and nonfinancial companies.  • Our affiliates include companies with a Neptune name; financial companies, such as Orion insurance; and nonfinancial companies, such as Saturn Marketing Agency.</td>
</tr>
<tr>
<td>Nonaffiliates</td>
<td>Companies not related by common ownership or control. They can be financial and nonfinancial companies.  • Nonaffiliates we share with can include mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations.</td>
</tr>
<tr>
<td>Joint marketing</td>
<td>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.  • Our joint marketing partners include credit card companies.</td>
</tr>
</tbody>
</table>
Meta-themes

Six meta-themes informed and guided the development of the prototype. To an extent, these meta-themes are universal design principles. The tendency in the design development of a complex product is to say too much, to let design decorate, to attract attention at the expense of balance, to provide the specifics without a context, and to standardize without discrimination. The final prototype—our design and content decisions—grows out of and is grounded in these themes, our particular research methodology, and our research results.

Keep it simple. Our research consistently showed that consumers are overwhelmed by too many words, complex information, and vague words and phrases. In fact, when faced with complex information, they often won’t even bother to read. Our evolution of the prototype focused on minimizing burden on the consumer by continually simplifying the notice. We stripped away redundancies, reduced words, used simpler words, clarified meaning, and provided key context information up front. At the same time, we did not oversimplify. A notice that strips away all contextual information will be short, but uninformative. The challenge is to
find the balance between as few words as possible and enough information so consumers understand.

**Good design matters.** Good design delivers important information in a format that reinforces the content. Our research repeatedly showed that consumers responded positively to the table design, headings, white space, bold text, bulleted lists, a larger font size, and full-size paper. These design techniques, combined with the simplified content, helped consumers better understand the information. They recognized that it looked different from other privacy notices, commenting that it was easier to read and that it looked more inviting. The easy-to-read design created the impression that the bank wanted the information to be read and understood.

**Careful design decisions ensure neutrality.** The point of privacy notices is to provide information, not direct a decision. They need to deliver information about financial sharing practices in a way that reports the information truthfully. We, therefore, focused on using factual language, objective presentation, and non-inflammatory words. In each round of testing, we listened for comments, reactions, and perceptions from consumers that indicated areas of potential bias in the notice. The iterative testing process allowed us to make design decisions that led to a final notice that is intended to be clear, neutral, and unbiased.

**A “whole-to-part” design is critical to comprehension.** Our research showed that consumers needed a context for understanding the information in the notice. Most consumers do not have an operational understanding of information sharing. Therefore, the notice needed to provide enough context that consumers could understand the detail both at the general level and at the table level.

The key frame component provides a context about financial sharing laws and personal information so consumers can understand the disclosure table.

The disclosure table frames the bank’s sharing practices by giving reasons financial institutions can share information. Consumers can then distinguish and understand the specific sharing practices of their bank and compare them to other institutions.

Consumers need the context of both the whole and part to understand the critical details. Without context, they understand virtually nothing.

**Standardization is highly effective.** Standardization of form and content helped consumers recognize the notice and the information in it. As they became familiar with the prototype, they learned where to look for the differences. Standardization reduces cognitive burden because consumers recognize the information without having to continually re-read notices word for word.
The disclosure table is critical. The disclosure table is at the heart of the prototype. It shows consumers how their personal information might be shared, how their particular bank shares it, and what sharing they can limit. Simple, concise, and highly visual, the standardized disclosure table simplifies highly complex and mandatory information into a design that consumers can understand without undue burden. Our research showed that consumers preferred the standardized disclosure table, could understand the disclosure information with greater ease than with the prose design, and could compare accurately sharing practices across financial institutions. The disclosure table, with its whole-to-part structure, is critical to consumer understanding and comparing financial sharing practices.

Ultimately, the prototype derived from eight rounds of testing ensures that the information about financial privacy laws and sharing practices is available to the public in a clear and understandable notice. This report extensively details the evolution of the prototype through each of the test rounds, illustrating how the prototype and its components clearly and conspicuously inform consumers, who can, therefore, make informed choices. That was the crux of the Form Development Project—and its success.
ANNEX D

“Ten Steps to Develop a Multilayered Privacy Notice”, Center for Information Policy Leadership
Ten steps to develop a multilayered privacy notice

Prepared by leading lawyers and experts in privacy with the Center for Information Policy Leadership
Foreword

Experts agree that good privacy begins with effective transparency. Transparency requires privacy notices that are easy to understand, facilitate comparison, and are actionable. Privacy notices must also comply with legal requirements that may differ from country to country, and jurisdiction to jurisdiction. Research on how people learn has shown that for notices to be easy to read and understand, they must be short, use plain language, and be presented in a common format. Complete notices tend to be longer and more complex, so it is impossible to have both sets of requirements in one document. A multilayered notice is made up of a condensed notice that contains all the key factors in a way that is easy to understand and is actionable, and a complete notice with all the legal requirements. A growing number of privacy officials and experts agree that multilayered notices meet the transparency objective. Corporate and government sponsored research shows that multilayered notices build both trust and compliance. The work of the European Article 29 Working Party gives us confidence that layering a privacy notice is legally compliant.

The purpose of this ten step guide is to help privacy practitioners in organizations of all sizes to assess their privacy notices and build effective multilayered notices, if appropriate.

After several years of testing and development, the international privacy community has begun to adopt multilayered privacy notices that make it easy for consumers to understand how their information is used and protected, and to compare companies' privacy policies. These new notices also encourage compliance and make it possible for organizations to use the same privacy notices worldwide. While there are still differences of opinion on notice content, we are at a point where organizations may feel comfortable using the notices discussed in this ten step guide to develop an easy to read and compare privacy notice, compliant with the emerging standard.

The guide begins with background on multilayered notices and a discussion of why you might like to change or update your notice. It then provides the reader with ten steps that can be followed by organizations of all sizes when developing multilayered privacy notices. Finally, the guide provides the reader with resources available on the internet for reference when developing a multilayered notice.

Background

With the growth of the internet in the 1990s, more and more organizations began publishing privacy notices. The complexity of the notices began to mirror the increasing complexity of information practices. Consumers found these notices confusing, and policymakers began to realize that the notices were failing to give the individual a clear picture of how their information would be used. Organizations had conflicting goals of creating notices that were easy to understand, complete, and compliant. By 2003, privacy leaders were beginning to discuss a concept called layered notices. A layered notice would be a short notice in a common template format, combined with a longer complete notice. This concept was endorsed by the 25th International Data Protection Conference, held in Sydney, Australia in 2003.

This basic concept was explored further at a workshop in Berlin in March 2004. The workshop, attended by data protection commissioners, other government officials, European consumer leaders and business, led to the Berlin Memorandum. The memorandum called for multilayered notices to be made up of as many as three layers. The additional layer would be a very short notice designed for use on portable digital devices, coupons and other places where space would be very limited. The Berlin Memorandum was discussed by the European Union’s Article 29 Working Party, which adopted a common position endorsing multilayered notices in December 2004.

The Australian Data Protection Commissioner recommended this evolving norm in a 2005 review of the Australian private sector privacy law. The Australian government subsequently adopted a layered notice
on its website. The Ontario Information Commissioner, working with the Ontario Bar Association, used layered notices as the basis for their new health care privacy notices. The US Postal Service adopted a multilayered notice in July 2005. The Data Protection Commissioners of New Zealand and British Columbia became the first Data Protection Agencies to publish condensed notices in November 2005.

Example

USPS notice

The first layered notices began appearing on US business websites in 2003. Companies began publishing multilayered notices in different languages in 2005. There are now condensed notices in over forty languages, including Arabic, Chinese, French, German, Korean, Japanese, Polish, and Russian.

This guide follows the recommendations in the European Union (EU) Article 29 common position of December 2004, which has gained wide acceptance within and outside the EU. This structure is as follows.

- Layer 1 - The short notice: the very minimum, for example, when space is very limited, providing only the identity of the data controller, contact details, and the purposes of processing.

- Layer 2 - The condensed notice: covering the basics in less than a page, ideally using subheadings, and covering Scope; Personal information collected; Uses and sharing; Choices (including any access options); Important information; How to contact us.
Why create a multilayered notice?

Privacy notices must be kept current. When updating the notice, organizations should strongly consider the multilayered approach. Multilayered notices are a big ‘win’ for organizations, consumers, and regulators.

Companies win because multilayered notices easily build consumer trust. Research conducted in Hong Kong, Germany, the United Kingdom, and the United States shows that consumers prefer the template-based condensed notice to longer text-based notices. The US Postal Service changed its notice when the template-based notice scored highest in a survey of public trust. Consumers like multilayered notices because they like information that is clear, graphically appealing, and easy to compare.

Companies also win because regulators in Europe and the Asia Pacific regions have agreed on the core concepts that need to be covered in short and condensed notices. This results in a single notice that can be translated into many languages, rather than a notice with different text for each country. This makes web notices much easier. P&G, MSN, and IBM have all published their web-based notices in more than 40 different languages.

Example

P&G French notice
Data protection authorities like multilayered notices because they increase public understanding of privacy and data protection — a clear goal for regulation. Many regulators also believe that multilayered notices will result in increased compliance with existing notice requirements. The bottom line is that all parties win when privacy notices are easy to read and understand.

Creating a multilayered notice

Creating a privacy notice should not be viewed as an intimidating process. Developing a multilayered notice is no more difficult than a full legally compliant notice. If an organization has already created a full legally compliant notice, they can skip the first 5 steps below and move directly to creating a condensed notice in step 6. Good practice principles would suggest a legal review before publishing any notice.

The ten steps

Step 1  Determine what your company does with personal data

Catalogue the organization’s collection, use, sharing, protection, and destruction of information that is about individuals. There are many means of doing this. You could start with the data and map its flows throughout the organization. You could also begin with the uses, and determine the data needed to fulfill those uses. An organization must understand its data flows before creating notices.

→ What personally identifiable data is collected directly from individuals, from transactions with individuals, or from third parties?
→ Where is that information collected?
→ How is the information used by the organization?
→ Is it shared with third parties? If so, with whom, and for what purposes?
→ How long is the information kept? How is it destroyed?
→ How is the information secured?
→ What choices does the individual have related to that use, retention, and sharing of information?
→ Does the consumer have opportunities to access and make corrections related to the information, either because of requirements in law or policy in the organization?

The OECD, the US Direct Marketing Association, and many other organizations have websites, guides, and online tools that may help you develop your full notice.

Step 2  Determine whether your company’s treatment of personal data is legally compliant

Review the laws, regulations, industry codes, contracts, and corporate promises that cover the collection and use of personally identifiable information to make sure the processes mapped meet legal expectations.

→ Is the data or use covered by law or industry codes of conduct?
→ Is there a contract in place to limit data use?
→ Is the data limited by consumers’ choices exercised either directly with the organization or with third parties?

→ Does the law require special notifications or disclosures to consumers? If so, how must those notifications or disclosures be addressed?

**Step 3  Develop and test an internal privacy policy that reflects how your company treats personal data**

Write an internal information policy to describe the processes. Make sure that the employees covered by the policy understand it.

→ The internal policy should match the organization’s culture. Write it in a way that matches the organization’s identity standards, bearing in mind plain language.

→ Test the policy with the legal department and other senior stakeholders.

→ Test with line managers to make sure the internal policy actually reflects corporate behavior.

→ Finally, test with employees to make sure they understand the policies. This testing should be done in a way that actually tests current compliance.

**Step 4  Use that internal policy to create the organization’s complete external privacy policy**

Make sure the external policy is consistent with the practices in step 1. This is the long, complete policy that meets all compliance requirements.

→ Have you included all the legal requirements in the complete notice? If you are using the complete notice in many countries, it might have special sections to address particular national requirements.

→ Have you included every significant use and sharing? Don’t forget to mention if you use outside vendors, agents, and processors.

→ Have you discussed information security? While the condensed notice doesn’t require a security section, almost all complete notices should.

**Step 5  Test and revise the full privacy notice**

Test the language and structure of the complete external policy to make sure it is understood by the target audience.

→ Is the long notice in language that most individuals would understand? Just because the notice is long doesn’t mean it should be hard to read. You should not need a university education to understand the notice. Keep the sentences simple and easy to read. Consistently use the same words to mean the same thing. This will also help translation.

Test the notice directly with consumers. This testing need not be costly. You can test a notice on your organization’s website. Once you have tested the notice you should revise it based on the research, and then retest.

**Step 6  Create the condensed notice**

Summarize the main elements of the complete policy in the six categories of the condensed notice. Use language that is easy to understand. If possible, take sentences directly from the full notice. This will help with consistency. You should compare the condensed and complete notices to make sure that
nothing has been left out of the condensed notice that is important or would be beyond the reasonable expectations of individuals.

→ **Scope**

Who is covered by the notice? The organization collecting the information? A family of companies? An entire industry? The scope should be defined clearly in as few sentences as possible. You should avoid long lists of affiliates - that detail should be in the longer notice.

**Example**

<table>
<thead>
<tr>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>This statement applies to XYZ company Web Sites Worldwide.</td>
</tr>
</tbody>
</table>

→ **Personal information collected**

This section should describe the types of information collected from the individual, from transactions with the individual, and from third parties about the individual. You should mention information gained from third parties such as credit bureaus or credit referencing services used to make decisions about the individual. You should also mention if you use cookies, if they are linked to personally identifiable information.

**Example**

<table>
<thead>
<tr>
<th>Personal information</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ We collect information you choose to provide during your registration.</td>
</tr>
<tr>
<td>→ We use common internet technologies, such as cookies and beacons, on our websites and emails.</td>
</tr>
<tr>
<td>→ We sometimes obtain additional information about you from other sources, such as your demographics and lifestyle information.</td>
</tr>
<tr>
<td>→ For more information about our information collection practices, please <a href="#">click here</a>.</td>
</tr>
</tbody>
</table>

→ **Uses and sharing**

This section discusses how the organization uses the information it collects. The organization should describe its own uses, uses by affiliated parties not listed in the scope, and non-affiliated sharing. The organization should list its own uses first, followed by affiliates and then non-affiliated third parties.

There has been a great deal of discussion about whether to mention sharing with vendors and agents in the condensed notice. Discussions with consumer, business, and data protection agency privacy leaders have led to a consensus that, in most cases, sharing with vendors and agents should be covered in the long notice. Any use and sharing that would be beyond the reasonable expectations of individuals, however, should be highlighted in the condensed notice.
Example

<table>
<thead>
<tr>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>We use personal information to provide you with information and</td>
</tr>
<tr>
<td>samples you request, and to help us develop new products and</td>
</tr>
<tr>
<td>services that meet your needs.</td>
</tr>
<tr>
<td>We do not share your personal information with other marketers</td>
</tr>
<tr>
<td>unless we have asked for and obtained your explicit consent. If</td>
</tr>
<tr>
<td>you do not provide your consent, we will not share your</td>
</tr>
<tr>
<td>information.</td>
</tr>
<tr>
<td>We will use personal information you provide only for purposes</td>
</tr>
<tr>
<td>consistent with the reason you provided it.</td>
</tr>
<tr>
<td>When we temporarily provide personal information to companies</td>
</tr>
<tr>
<td>that perform services for us, such as to send you email or samples,</td>
</tr>
<tr>
<td>we require those companies to protect the information in the</td>
</tr>
<tr>
<td>same manner as XYZ. These service companies cannot use your</td>
</tr>
<tr>
<td>personal information for any other purpose than the reason you</td>
</tr>
<tr>
<td>provided it to XYZ.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section would include choices the individual has relating to</td>
</tr>
<tr>
<td>the information collected and used. In some instances the choices</td>
</tr>
<tr>
<td>are consents, while in other instances they are opt-outs. In many</td>
</tr>
<tr>
<td>jurisdictions the consumer has the right to request access to</td>
</tr>
<tr>
<td>information and request corrections or deletions. These choices</td>
</tr>
<tr>
<td>should be in this section.</td>
</tr>
</tbody>
</table>

Example

<table>
<thead>
<tr>
<th>Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>You may access personal information that we hold about you. You</td>
</tr>
<tr>
<td>can ask us to correct any errors or delete the information we have</td>
</tr>
<tr>
<td>about you.</td>
</tr>
<tr>
<td>You may opt-out of any further contact from us.</td>
</tr>
<tr>
<td>To protect your privacy and the privacy of others, we may have to</td>
</tr>
<tr>
<td>verify that you are who you say you are before we can give you</td>
</tr>
<tr>
<td>access to, or change, information about you.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every organization has factors unique to its management of</td>
</tr>
<tr>
<td>personally identifiable information. Some organizations have seal</td>
</tr>
<tr>
<td>programs, while other organizations have special protections for</td>
</tr>
<tr>
<td>information. This section is where organizations would place</td>
</tr>
<tr>
<td>seals and other important facts. You could also mention special</td>
</tr>
<tr>
<td>legal requirements in a particular jurisdiction, or information</td>
</tr>
<tr>
<td>about where a person can complain.</td>
</tr>
</tbody>
</table>
Example

Important information

BBBOnline reviews and enforces our compliance with this privacy notice. XYZ participates in the EU/Department of Commerce Safe Harbor Program.

→ How to contact us

The last section gives the individual information on how to contact the organization for a complete notice, to ask questions, and to exercise choices. Many organizations give the individual more than one way to contact the organization.

Example

How to contact us

E-mail: privacy@xyz.com.

By post: XYC, Privacy Office, 475 Morningside Drive, Rochester, NY 12345.

To see our full privacy policy, click here.

Step 7  Harmonize the full and condensed notices together

Now that you have developed the condensed notice it is time to go back and look at the full notice to see if there are any format changes to make them consistent. In some countries, many consumers will want to see the full notice. The complete and condensed notice must work together whether the complete notice will be available from a click-through on-line, or on request off-line.

→ Does the complete notice need to be reorganized so that topics are in the same order as the condensed notice?

→ On-line, do you want to hyperlink the complete and condensed notice?

→ Are there words and phrases that need to be made consistent?

→ Do the two notices reflect the same organizational identity?

Step 8  Create the short notice

If the organization collects information over a hand-held computer, mobile phone, or with coupons, you should now develop the short notice for these applications.

The short notice must contain three items of information.

→ Who is collecting the information?

→ What is the primary use for the information? You should also include non-primary uses that would be beyond the reasonable expectations of the consumer.
Step 9  Review and test the multilayered notices

It is important to see whether the target audience understands how the three layers work together. This may be through consumer research on your website. Finally, you should read through the notices again to make sure that there is nothing in the complete notice that would be beyond the reasonable expectations of the consumer, that has been left out of the condensed notice. In some jurisdictions, this lack of consistency might be perceived as deliberate deception.

- Do the layers work together?
- Are there important facts that have been left out of the notice?
- Are all the notices consistent? Would the reader be surprised reading the full notice after reading the condensed notice?

Step 10  Publish your new multilayered notice

Make sure the various layers are published in the correct locations. All employees with consumer contact must be aware of the notice layers and how to provide a complete notice when asked.

- Have your consumer affairs staff been educated on the various notice layers?
- Can they explain your policies to the intended audiences?
- Have you placed the various layers where they legally must be placed, as well as where you want them placed to build trust?

Resources

For more information and for the documents referenced in this paper, please visit the Center for Information Policy Leadership at www.informationpolicycenter.com. You will also find useful information at:

1  Direct Marketing Association Privacy Policy Generators
   www.the-dma.org/privacy/privacypolicygenerator.shtml

2  BBBOnLine
   www.bbsonline.org/reliability/privacy/

3  OECD Privacy Statement Generator
   www.oecd.org/sti/privacypolicy.html
Portfolio of condensed notices

Government of Australia
Portfolio of condensed notices

For more information, read our Full Privacy Policy.

PERSONAL INFORMATION
- We get information from your requests for our products or services. One example is income on loan applications.
- We get information about your transactions with us and with others. For example, we have your account balance information.
- We get information, such as your credit history, from credit bureaus.

SCOPE
- These statements apply to the Chase and Bank One family of companies owned by JPMorgan Chase & Co. and to our customer customers.

USES
- We manage information to serve you.
- We may share information about you within our family to offer you financial products and services.
- We may share information about you with outside companies that work for us. These may include firms that assist in marketing our products.
- We may share information about you with outside financial companies to allow you the opportunity to receive additional products or services.
- We may share information about you outside of our family as permitted by law, including our service providers, credit bureaus and law enforcement.

YOUR PRIVACY CHOICES
- You may tell us not to share information about you with non-financial companies outside of our family of companies.
- You may tell us not to share certain information about you within our family of companies.
- To make any of these choices, submit your privacy choices online or contact us at 1-800-325-3304.

IMPORTANT INFORMATION
- Review helpful information on identity theft or how to get help if you become a victim.
- View our online consumer information practices.
- View the Privacy & Security FAQs.
- Some states have different privacy provisions.

HOW TO REACH US
- Contact us via email or by calling 1-888-888-8888.
- Submit your privacy choices online.

For more information, read our Full Privacy Policy.

This site is dedicated at persons in the United States only. Persons outside the United States may visit International Banking.
Portfolio of condensed notices

MSN (Japanese)

【個入情報の関与】

- MSNでは、お客様がMSNのサービスに提供する個人情報、個人情報に個人情報を利用しています。
- 携帯電話情報は、ももMicrosoft Corporationのサービスおよび個人情報から取得した書類を保護することもあります。
- MSNでは、携帯電話にメールのサービスの有効性を記録し、携帯電話とのサービスを受けるために、Cookieおよびその他の技術を使用しています。

【オプション】

- お客様とMSNとの連携方法を変更するには、「MSNプライバシー設定」にアクセスしてください。
- ユーザーのメール設定の変更が必要な場合、最新の設定を承認するには、HotmailおよびOutlook Expressの設定ページにアクセスしてください。
- 購読するMSNニュースリーダーについては、newsletters.msn.comにアクセスしてください。

【個人情報の管理】

- 郵件のMSNサービスに関する情報については、プライバシーやサービスに関する内容を守るために、必要とする情報量を最小限に抑えます。
- MSNの通信サービスおよびオンラインサービスには、Microsoft Passport Networkを有しています。Passportサービスの詳細については、Microsoft Passport Networkプライバシーやサービスに関する詳細を読みください。
- 本プログラムのプライバシーやサービスの詳細については、プライバシーやサービスに関する内容を守るために、必要とする情報量を最小限に抑えます。
- お客様のコンピュータ、電話機、個人情報、およびご契約人のオンラインコミュニケーションに関する情報に関する詳細については、「コンピュータのプライバシー設定」を読みください。

【プライバシーに関する明示】

MSNのプライバシーやサービスに関する詳細については、http://privacy.msn.comにあるプライバシー設定をご覧ください。
Portfolio of condensed notices

IBM (Slovenia)

Zasebnost

IBM-ovi postopki za varovanje zasebnosti na spletu

Osebno informacijo

Na internetu nas lahko obiščete brez identifikacije ali podajanja osebnih informacij. Občasno pa bomo od vas morda zahtevali informacije, na primer: za obdelavo naročila, za odpravo informacij na zahtevanje, za zagotavljanje naročnina ali v zvezi z vso proiznjo za delovno mesto. Te informacije lahko dopolnimo z izvedbo transakcije ali za udobnost boljših storitev.

Uporaba

- Za izpolnitev vaših zahtev iz naše strani ali strani drugih, ki so vključeni v izpolnitev.
- Za vzpostavitev v stiku z vami za enake o zadovoljstvu stranik, za reziskovanje trga ali v povezavi z vključenimi transakcijami.
- S strani IBM-ovih izbranih organizacij za namene trženja, glede na to, kako uporabnik polegali.
- V nadobljivih oblikah za analizo (npr. podatki o potekih obiskov spletnih strani).
- Za razvoj našega poslovnega odnosa, da predstavljate IBM-ovega poslovnega partnerja ali prodajalca.

Vaše izbire

- Ko zbiramo vaše informacije, nam lahko poveste, da ne želite, da so le-te uporabljene za nadaljnje trženje, in vaše želje bomo upoštevali.
- V sklopu naših izbiralnih politik.

Posebnostne informacije

IBM je člen programa TRUSTe (www.truste.org). IBM upošteva dolžioca vključenega v spletne stranice Safe Harbor med EU in ZDA. Za potravljanje nezaveznosti v IBM-ovem zapisu vaših osebnih informacij se obrnite na podatkovne informacije ali IBM na access_request@us.ibm.com.

Za celotno IBM-ovo obvestilo si oglejte IBM-ovo pravilnik o zasebnosti.
Portfolio of condensed notices

Lenovo (German)

Datenschutz
Umgang mit den Lenovo Datenschutzbestimmungen im Web

Persönliche Informationen
Im Normalfall können Sie unsere Internetseiten aufrufen, ohne irgendwelche Angaben über Ihre Person zu machen. Im Einzelfalle benötigen wir jedoch Informationen von Ihnen, beispielsweise um mit Ihnen zu korrespondieren, um einen Auftrag auszuführen, um ein Abonnement abzurufen oder wenn Sie sich auf eine Stellenausschreibung bewerben. Gegebenenfalls beziehen wir Dritte ein, um eine Transaktion auszuführen oder um einen besseren Service anbieten zu können.

Verwendung Ihrer Daten
- Zum Ausführen Ihrer Anforderungen durch uns oder durch in die Auftragsabwicklung einbezogene Dritte.
- Um Sie im Rahmen einer Umfrage zur Kundenzufriedenheit oder für Marktforschungszwecke oder in Verbindung mit einer Transaktion zu kontaktieren.
- Für Marketingzwecke von Lenovo und ausgewählten Dritten, wenn Sie zugestimmt haben, dass Ihre Daten für solche Zwecke verwendet werden dürfen.
- Als anonyme Informationen zur Analyse (z. B. Click-Stream-Daten).
- Zum Bau von Geschäftsbeziehungen, wenn Sie ein Lenovo Business-Partner oder Lieferant sind.

Ihre Auswahlmöglichkeiten
- Wenn wir Daten von Ihnen erfasst haben, können Sie uns auffordern, diese Daten nicht für weitere Markenkontakte zu verwenden. Dieser Wunsch werden wir respektieren.
- Sie können die Cookies in Ihrem Browser deaktivieren.

Wichtige Informationen
Um falsche Angaben im Lenovo Datensatz mit Ihren persönlichen Daten zu korrigieren, kontaktieren Sie den Absender.

Die vollständige Lenovo Erklärung finden Sie unter Lenovo Datenschutzbestimmungen.