

Title: Become a Privacy-Positive Organization

Date: 26th July 2001

Is customer privacy a threat or opportunity? Organizations that succeed in pleasing customers know how to balance privacy and personalization. Two organizations offer six guidelines to get on the right privacy track.

Can you offer personalized service and still enforce privacy?

Yes!

Some customers are happy to release personal data when they know it results in desirable product and service offerings

The privacy challenge

For many businesses, new economy or old, the deciding factor between success and failure is how effectively they market. Consider the saying: "Half the money I spend on advertising is wasted; the trouble is, I don't know which half." Despite advances in technology, this is still a truism with which a lot of companies agree (even as academics still argue over who said it-- Philadelphia department store magnate John Wanaker or British Viscount Leverhulme, the man who put the lever in Unilever). Regardless of who said it, we can all agree that any company that halves its advertising budget without reducing the effectiveness of its marketing efforts will see a boost in profitability.

Some businesses conclude that the most effective way to spend marketing dollars is to target them, making sure they're spent on the people most likely to respond positively. Some might even argue that these days we do know where the wasted half of the advertising dollar is spent: on people who aren't interested to begin with. The challenge of how to find the people most likely to respond is also at the heart of the privacy challenge. You can't tell if someone is likely to be interested in your product unless you know something about that person, and it follows that the more you know, the better you're able to target that customer with advertising dollars.

For some of today's consumers this is a welcome fact of online life. They get offered good deals on things they actually want. They get services tailored to their circumstances. And if giving out more information about their preferences and lifestyle would result in fewer solicitations for things they don't want, many consumers could consider giving out that information if they trusted the parties to whom that information was given. This brings us to today's privacy paradox: People want personal service and preferential treatment, but they're reluctant to share their personal information and preferences.

This paradox isn't confined to online business and the Internet economy, but it's where the paradox is most apparent, precisely because the Internet enables a high degree of targeting and customization, **IF** the target is prepared to reveal personal preferences and demographics.

Reality check: This is a big if. Numerous surveys have shown that only a small percentage of today's consumers have a high degree of trust when providing personal data to Web sites. A recent Gallup poll indicated more than three quarters of Internet users were concerned about privacy, and very few were willing to give

out personal information. A different study found only 6 percent of consumers have a high degree of trust when providing Web sites with personal data.

Real-world mishaps

Is this distrust justified? Consider what happened this summer at Eli Lilly, one of the world's largest pharmaceutical companies. One of Lilly's biggest revenue producing products is Prozac, widely prescribed as treatment for depression, bulimia, or obsessive-compulsive disorder. Two years ago, Lilly decided to offer an e-mail service to help Prozac takers stick with their regime, and to establish a more intimate relationship with its customers. Customers who signed up received regular e-mail reminders to take their medication, but in June 2001, Lilly decided to discontinue the service. Lilly's patent on Prozac expired in August 2001, and they only had 600 subscribers out of the millions of people taking the drug. An e-mail message was sent out in June 2001 to inform subscribers of the decision. Unfortunately, the e-mail addresses of all 600 subscribers were clearly readable to all recipients in the "cc" field.

News of this privacy breach was widely reported in the press, which regularly covers the public's anxiety and ambivalence about the issue of privacy vs. personalization. Eli Lilly issued a statement saying the slip-up was the result of a programming error and that the company greatly values customer privacy. But that didn't appease some vocal critics, who talked of legal action, government investigation, and regulatory sanction. And it probably did little to reverse the public perception that Lilly could be trusted to keep private data private.

Bear in mind that nobody accused Eli Lilly of intentionally breaching privacy, not even the fiercest privacy advocates. And nobody claimed that this was a breach of company security. No security measures were undermined by hackers or disgruntled employees. The complaint was that the company didn't exercise enough care when handling sensitive information.

Consider: This points to an important connection between business goals and IT execution of those goals. What a company avows as policy, it must execute in practice. Many companies have made important strides in this area with respect to other aspects of their business, such as customer service and data security. When companies internalize their commitment to these objectives, call center response times and network perimeters are monitored and managed. But taking to heart the implications of a commitment to privacy takes time.

For example, the incident at Lilly could be categorized as a quality control issue. It certainly would appear that there weren't enough quality checks in place to prevent a classic e-mail error--mass mailing to a list with the cc function instead of bcc (a good argument for avoiding this method of mass mailing altogether). Those checks might have been in place if the significance of an error had been better understood. And while nobody is accusing Lilly of not having a privacy policy, the depth of the company's commitment, called into question by this one error, was subject to further skepticism when people noticed that the main page at the corporate Web site had no links to privacy.

Rise to the challenge

Clearly, companies who say they value privacy must internalize what this means in practice, and privacy commitments have to be documented. This is no small task, but for companies in some fields, this is no longer optional. In the United States, privacy regulations are coming into force for industries such as healthcare and financial services, and international privacy regulations are starting to impact a wide range of industries. When Forrester Research recently examined the U.S. Fortune 100, it concluded that 73 are already required to comply with at least one of the federal privacy regulations that became law in the last two years. And more are on the way. In just a two-year span, Congress introduced nearly 1,000 bills on Internet privacy and spam, which includes unsolicited commercial e-mail or UCE, which is considered a form of privacy invasion by many Internet users.

In the United States there are also state laws to consider. For example, on spam alone, 18 states now have constructive laws. As of March 2001, there were 314 privacy-related bills pending in 42 states, and 36 Internet-specific privacy bills in 11 states, along with 14 identity-theft bills and 51 various financial privacy bills. And trading partners such as Canada, Australia, the European Union, and parts of Asia are requiring different levels of privacy protection. Many of these are based on the Data Privacy Principles developed by the Organization for Economic Cooperation and Development (OECD.) The OECD has made efforts to ensure the free flow of economically necessary personal information by proposing standards that would harmonize different national data protection and privacy legislation schemes.

Smart move: If you want to assess the status of your privacy commitment, review the OECD principles. They represent what consumers worldwide are demanding of companies, which gives them a relevance that goes beyond specific legislative measures in the United States. U.S. regulations are likely to seesaw for some time between privacy advocacy and corporate objections based on cost and restraint of trade.

How to succeed

There are three different options on privacy today. Your company can be privacy negative, doing nothing and trying to ignore the issue. This is impossible in certain industries, and increasingly difficult in any industry if you do business outside the United States. Your company can be privacy neutral, doing the bare minimum to meet legal requirements and considering that expenditure a waste of money imposed by excessive government regulation.

Or your company can be privacy positive. Make a privacy commitment and prove you can deliver on it. Do this by documenting your privacy policy and your compliance with it by meeting or exceeding all government regulations, and by minimizing violations of policy and regulations. Make privacy a consideration in all aspects of the business, from advertising at the front end, to IT systems on the back end.

Success factors: Being privacy positive accomplishes three important goals for your company:

- 1)** You get to boast about your commitment to privacy, which is proving to be a valuable market differentiator.

- 2) You gain immunity from privacy negatives, such as prosecutions, fines, stings, and slip-ups. (If privacy lapses do occur, your positive stance provides an easier recover).
- 3) You get closer to customers, who trust you with more of their personal data and preferences, helping you target, and thereby maximize, your marketing dollars.

Data Privacy Principles

These principles developed by the Organization for Economic Cooperation and Development (OECD) are an important starting point or benchmark for any organization's data privacy practices, since many countries are using them as the basis of data privacy laws.

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures that give effect to the principles stated above.

Six Resolutions for Responsible E-Mailers

These resolutions, adopted by the Council for Responsible E-mail (CRE), are useful guidelines for any organization that uses e-mail for marketing purposes, a critical arena for privacy concerns.

1. The CRE agrees that marketers must not falsify the sender's domain name, or use a non-responsive IP address without implied permission from the recipient or transferred permission from the marketer.

2. The CRE agrees that marketers must not purposely falsify the content of the subject line or mislead readers from the content of the e-mail message.

3. The CRE agrees that all bulk e-mail marketing messages must include an option for the recipient to unsubscribe (be removed from list) from receiving future messages from that sender, list owner, or list manager.

4. The CRE agrees that marketers must inform the respondent at the time of online collection of the e-mail address for what marketing purpose the respondent's e-mail address will be used.

5. The CRE agrees that marketers must not harvest e-mail addresses with the intent to send bulk unsolicited commercial e-mail without consumers' knowledge or consent. (Harvest is defined as compiling or stealing e-mail addresses through anonymous collection procedures such as via a Web spider, through chat rooms, or other publicly displayed areas listing personal or business e-mail addresses.)

6. The CRE opposes sending bulk unsolicited commercial e-mail to an e-mail address without a prior business or personal relationship. (Business or personal relationship is defined as any previous recipient-initiated correspondence, transaction activity, customer service activity, third-party permission use, or proven offline contact.)