A primer for customer privacy management

Walter Janowski takes a US perspective on how organisations should implement a compliance programme for managing customers' privacy preferences.

Economic pressures are driving enterprises to search for ways to squeeze maximum returns out of their customer relationships, and along the way some enterprises are testing just how much intrusion customers will tolerate. Whether or not these efforts violate enterprises' own privacy policies, they can result in a backlash from customers, privacy advocates and the media.

As enterprises become more aggressive in their marketing efforts and seek ways to circumvent privacy restrictions, the potential for a high-profile privacy-abuse scandal increases. In a climate where the general public is greatly concerned with corporate ethics and accountability, an enterprise that makes a significant misstep in managing its customers' private information could become the "Enron of privacy".

In addition to the potential damage to the enterprise's reputation and brand, it is likely that such an event would drive US government regulation to enact more restrictive privacy legislation along the lines of what has been implemented in the European Union. By 2005, at least one major US enterprise will experience high-profile customer backlash due to the mismanagement of customer privacy information, and public outcry will motivate the US Congress to mandate restrictive privacy legislation.

Given the current state of the economy, privacy management must be prioritised with other investments. Without a serious public breach to serve as a warning, privacy management likely will continue to receive low priority. Thus, when the abuse of customers' personal information by an enterprise leads to a highly visible, public scandal, enterprises will be ill-equipped to respond. Although enterprises cannot forecast the shape that government privacy legislation could take, those that address privacy management concerns today will not only be ahead of their competition, but will also be better prepared to accommodate privacy legislation requirements when they appear.

Without a serious, public breach to serve as a warning, privacy management likely will continue to receive low priority. Thus, when the abuse of customers' personal information by an enterprise leads to a highly visible, public scandal, enterprises will be ill-equipped to respond.

THREE CRITICAL COMPONENTS OF PRIVACY MANAGEMENT

For any enterprise, crafting a comprehensive privacy policy for managing customer data is an important first step in implementing customer privacy management. However, how that policy is implemented and used throughout the enterprise is every bit as important as the policy itself. Here, we define the three critical components of customer privacy management as being able to communicate, enable and enforce a privacy policy.

Communicate — Privacy preferences at the individual customer level must be determined, recorded and distributed where appropriate. Customers may select "opt-in/opt-out" preferences that are applicable enterprise-wide or specific to particular types of communications or channels. Customers also must be able to view and understand an enterprise's privacy policies. They must be able to regularly access their profiles, view their preferences as recorded by the enterprise, and change/maintain these profiles as required. Once collected, the complete set of preferences for each customer must be communicated enterprise-wide, wherever a customer communication might occur. Although the consolidation of customer information into a single data repository is preferable, for many enterprises, customer data is so fragmented enterprise-wide that it would be prohibitive to delay privacy initiatives while waiting for consolidation. In such cases, interactions between databases must be structured so that privacy preferences can be managed from a single access point, but are available wherever customer data is accessed.

Enable — Once customer privacy preferences are established, mid-level marketers should not make decisions as to which customer profiles they can access as marketing prospects. The internal distribution of customer information must be managed by a central, higher-level role (for example, senior marketing manager or chief privacy officer), and must be based on the individual privacy preferences specified by the customers. For example, if a marketer prepares an e-

mail marketing campaign, he should not be able to query the entire customer database to determine e-mail preferences to prepare his customer target list. Instead, he should only have permission, from a more-senior level, to access names of customers who have granted e-mail access.

Enforce — Once implemented, an enterprise's privacy policy is useless if its employees don't follow it. Enterprises must implement processes and monitoring technologies to ensure that policies are properly enforced. This can be partly accomplished by restricting data access. However, enterprises also must be able to detect rogue internal initiatives (for example, a department that creates a customer database through independent customer contact) as well as to monitor potential abuses that are technically "within the law" of a privacy policy (for example, a customer who has given permission to be contacted by e-mail becomes the target of an aggressive daily e-mail bombardment).

PRIVACY CHECKLIST

Within the realms of these three critical components, we define a checklist of eight key considerations in privacy policy implementation (see chart below).

Many enterprises consider a privacy policy as an end rather than a beginning. However, once a comprehensive privacy policy is crafted, the challenge of implementation becomes apparent.

COMMUNICATE

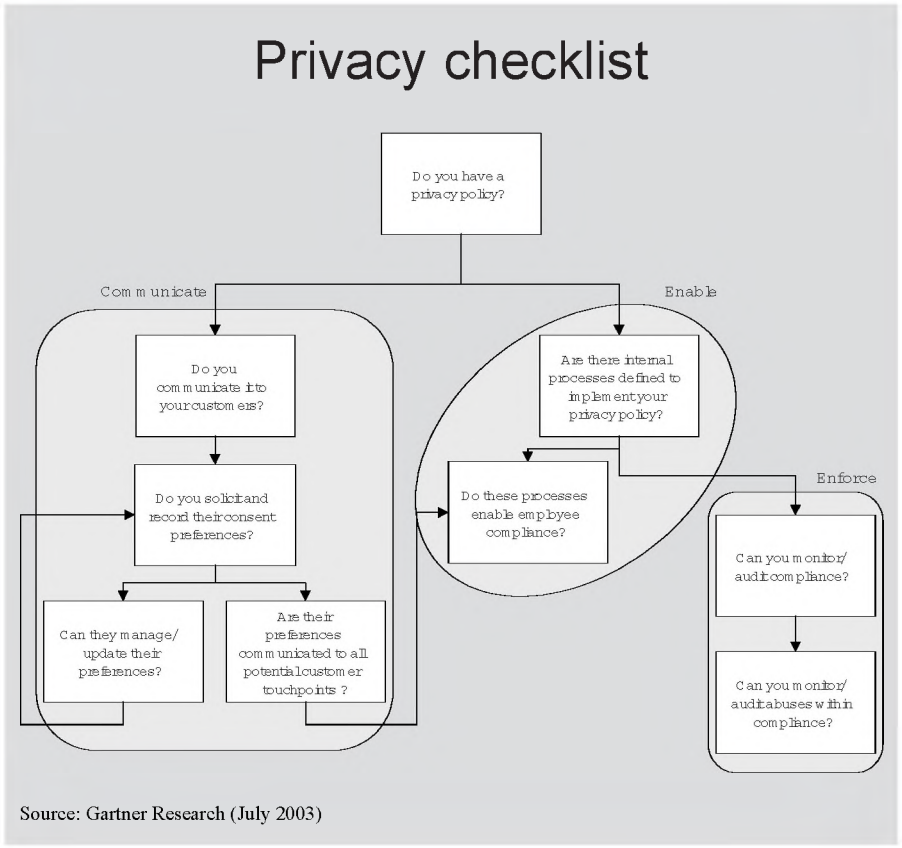
Do you communicate your privacy policy to your customers? Obviously, your privacy policy is of no use to your customers if they cannot see it. How is it presented to them? Is it easily accessible? Mailing a tiny, multipage pamphlet filled with fine print and legal terminology may fulfil the technical requirement for customer notification, but it does little to instill customer trust or confidence. Customers should have the opportunity to access your privacy policy anywhere and anytime they want it. Make it accessible from your website and provide copies wherever and whenever there is a customer interaction. The overriding goal is to make it available when it is needed, and it should not be the customer's responsibility to capture and retain it when you choose to send it.

Do you solicit and record your customers' consent preferences? The two requirements in communicating your privacy policy to your customers are commonly known as notice and consent. Although making your privacy policy available to them provides notice of how you plan to handle their data, you must also solicit their consent to your intentions.

Whether your approach is to ask for opt-in (for example, "Here's what we plan to do, but only if you agree") or opt-out (for example, "Here's what we're going to do unless you tell us not to"), it is necessary to have a process in place to collect and retain customer responses indicating their preferences about how you handle their data. The more flexible your privacy policy and the more specific choices you provide for your customers, the more complex the process of collecting and maintaining these preferences will be.

Can your customers manage and update their consent preferences? A customer's privacy preferences are not static, and provisions must be made to allow for changes over time. A customer may grow weary of frequent bombardment with offers and choose to opt-out from future contact, or an interested customer may choose to opt-in to a new offering. Customers must have the ability to review the choices they have made in response to your privacy policy and be able to revise those choices as they please. Although this is commonly enabled via the company website, the process should be designed for the customer's convenience, and it should also be accessible by phone, by mail, in person or through whatever channel the customer prefers to use to communicate with the enterprise.

Are your customers' consent preferences communicated to all potential customer touchpoints? Once your customers' preferences are collected, how do you "spread the word"? Everywhere within the enterprise where there may be an opportunity for customer contact, those preferences must be accessible. When the customers express their preferences, they expect that it should only need to be done once. It is the



Source: Gartner Research (July 2003)

responsibility of the enterprise to collect those preferences wherever the customers might choose to present them, and to make sure that those preferences are communicated across the enterprise wherever a customer contact might occur.

ENABLE

Are there internal processes defined to implement your privacy policy throughout the enterprise? Processes must be in place to control the way customer data is handled within the enterprise once it is collected. The privacy policy explains what you need to do; the processes will dictate how you do it. An enterprise-wide memo that says "everyone must read the privacy policy and follow it" is not enough. A proper approach would be to perform a business process audit to identify every potential activity in which customer data is accessed and used. Then, assess each process to determine the appropriate controls to be put in place. In addition, if enterprise partners have access to any enterprise customer data, processes must be in place to ensure that they comply with the enterprise privacy policy as well.

Do these processes enable employee compliance? Once customer privacy processes have been established, employees should not need to make decisions about which customers they can access as prospects. When the internal distribution of customer information is managed by a central, higher-level role (for example, a senior manager or chief privacy officer), employees should only have permission, as dictated by that more senior level, to access names of customers who have granted contact permission.

If an employee is overstepping his or her authority and abusing customer data outside the limitations of the privacy policy, can you detect it before the customer complaints start coming in?

ENFORCE

Can you monitor and audit compliance with your privacy policy? Your privacy policy is completed and communicated to your customers, you are collecting customer data and their consent preferences, your processes are in place, and your employees have been trained and educated. How can you be sure that everything is in place and running smoothly? There must be methods in place to ensure that all privacy communications are occurring smoothly, and that processes are being followed as defined. If an employee is overstepping his or her authority and abusing customer data outside the limitations of the privacy policy, can you detect it before the customer complaints start coming in?

If customers challenge that their data has been misused, can you prove that they were appropriately notified, that their preferences were collected, and that their data has only been accessed and used within the terms of your policy? An audit trail must be in place that records the details of all customer communications surrounding their consent preferences, along with data monitoring of who accessed the data, when, and for what purpose.

Can you monitor and audit abusive practices within the guidelines of your privacy policy? Even with appropriate compliance in place, it is still possible to abuse the privileges afforded by your privacy policy. For example, even though a customer may have opted-in to be contacted with offers about new products, that does not necessarily mean that he or she would appreciate receiving 20 new offers every day. Even within the definition of your privacy policy, there must be specific guidelines in place within the enterprise to control how customer information will be used, and you must be able to monitor and audit how those customer permissions are being used or abused.

BOTTOM LINE

When an enterprise is judging whether a particular business activity is effective, ethical or even legal from the perspective of customer privacy, the answer is simple. An enterprise can do anything it wants with a customer's data, as long as the customer has been informed of it and has consented to it. Although simple in concept, the processes and technologies required to communicate, enable and enforce that consent form a complex web of activities within an enterprise. To ensure total compliance with its privacy policy, an enterprise must effectively address all eight of the areas of the customer privacy management checklist.

Three Steps to Privacy Management

- Communicate customer privacy preferences to all necessary parties within your organisation.
- Enable access to customer data to senior level managers for appropriate distribution of data.
- Enforce privacy policies vigorously with stringent processes and monitoring technology.

AUTHOR: Walter Janowski is research director with Gartner's CRM Research practice and an IAPP member. He can be reached at: Tel: +1 203 316 1266, E-mail: bizapps@gartner.com.

This article first appeared in the *Privacy Officers Advisor* and is reprinted by permission of the International Association of Privacy Professionals, www.privacyassociation.org.