

Managing Conflicts of Customer Insight and Privacy in CRM

Walter Janowski, Claudio Marcus

To be successful at customer relationship management, enterprises must understand how to achieve an appropriate balance between developing customer insight and maintaining customer privacy.

ANALYSIS

There's an inherent conflict today in using customer information for customer relationship management (CRM). On the one hand, enterprises have access to more customer information than ever before. Today's technology allows enterprises to collect more customer data at an increasingly faster rate and to consolidate customer data from disparate databases. Enterprises can then analyze this data to gain insights into customers' behaviors and needs. Such analysis enables enterprises to deliver marketing offers, product offerings and service levels that better align with customer value (or potential value) and customer expectations.

On the other hand, enterprises that engage in this kind of information gathering risk customer backlash if customers perceive that their personal privacy is being violated. Since Sept. 11, governments have begun to collect and monitor more personal information than ever. This, in turn, has accelerated an already existing trend among the general public to control and protect personal information wherever possible — such as in business transactions. To succeed at CRM, enterprises must understand how to achieve an appropriate balance between developing customer insight and maintaining the customer's sense of privacy. Aside from doing what's legally and ethically right, enterprises must be equally concerned with an individual customer's *perception* of how his or her privacy is being managed.

At the same time, economic pressures are driving enterprises to search for ways to squeeze the maximum returns out of each customer relationship. Many enterprises are testing just how much intrusion their customers will tolerate. When faced with questions of whether a particular business activity is effective, ethical or even legal from the perspective of customer privacy, the answer is simple, although sometimes hard to face: 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.*

Unfortunately, the need to get consent means that some percentage of customers will deny that consent. Consequently, many enterprises wrongly look for ways to bypass this step, leading to ill feelings on the part of their customers.

However, the need to comply with customers' privacy preferences can work to your advantage. Marketers have used segmentation techniques for years to differentiate the offers and interactions they have with different customer groups. Today, along with providing traditional data, your customers are telling you something very important about themselves when they tell you how they want you to handle their data. In "When It Comes to Privacy, One Size Doesn't Fit All," DF-16-3132, Scott Nelson suggests ways to use customers' privacy preferences to segment the ways in which you develop your interactions with those customers.

Some enterprises have tried to work around the personal information restrictions they or their customers have put in place. Even when these work-arounds haven't technically violated an enterprise's own privacy policies, they have often resulted in customer and media backlash. In "Worst Practices in Customer Privacy Management," TU-16-6918, Walter Janowski looks at how some well-known companies have tried — to their eventual regret — to test the limits of privacy and how to avoid falling into those traps.

Once customers have opted out of receiving communications from your enterprise, it's unlikely they will return unless you give them good reason. In "Five 'Privacy Protecting' Ways to Encourage Opt-In," TG-16-6693, Adam Sarner explores some techniques that can be used, without setting off alarms of potential abuse, to entice your customers to reconsider their position.

As part of a holistic approach to CRM, enterprises are looking to deliver more-effective post-sale interactions with their customers through proactive customer service. Although generally considered a marketing issue, customer information privacy is also a critical consideration for

customer service. To reach out and interact with your customers and their service needs, you need to collect and manage personal information about your customers, along with their transaction history with your organization. In "Privacy in Personalized Customer Service," COM-16-6941, Esteban Kolsky considers best practices for handling those customer privacy issues from a service perspective.

A well-defined privacy policy is a must-have, but it is little more than an empty promise without policies and processes in place to secure the data and ensure employee compliance. Such policies are challenging enough to maintain within the four walls of your enterprise; today's mobile workplace delivers customer data outside the physical office to employees traveling or working at home. In "CRM-Related Privacy Concerns in the Remote Workplace," SPA-16-3010, Richard DeLotto takes a look at the risks associated with employees who deal with customer data in the remote workplace, and what enterprises can do to minimize those risks.

Features

"When It Comes to Privacy, One Size Doesn't Fit All" (DF-16-3132). Don't assume all customers have the same attitude about privacy. **By Scott Nelson**

"Worst Practices in Customer Privacy Management" (TU-16-6918). Resist the temptation to sidestep the restrictions of your own privacy policies. **By Walter Janowski**

"Five 'Privacy Protecting' Ways to Encourage Opt-In" (TG-16-6693). Be creative to avoid consumer opt-out of permission-based e-mail. **By Adam Sarner**

"Privacy in Personalized Customer Service" (COM-16-6941). Ensure that customer privacy remains a priority, even in unusual situations. **By Esteban Kolsky**

"CRM-Related Privacy Concerns in the Remote Workplace" (SPA-16-3010). Audit your remote-workplace practices to avoid breaching consumer privacy or corporate confidentiality expectations. **By Richard DeLotto**

This research is part of a set of related research pieces. See "CRM Demands Sound Customer Privacy Practices" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509