SPRING 2013 VOL.54 NO.3

MITSloan Management Review

Intelligence

Why Managing Customer Privacy Can Be an Opportunity

A brief discussion of three strategies companies can use to manage privacy policies in a manner that will provide a positive customer experience, by Avi Goldfarb and Catherine Tucker

REPRINT NUMBER 54309

[CUSTOMER SERVICE]

Why Managing Consumer Privacy Can Be an Opportunity

Too often, companies treat privacy policies as a compliance cost. Instead, think of managing consumer privacy as a way to give people a positive experience with your brand.

BY AVI GOLDFARB AND CATHERINE TUCKER

How many privacy policy updates does your credit card company send you each year? How many of them do you read through — and how many get immediately trashed? Companies often "manage privacy" and "keep consumers informed" by drafting their privacy policies as broadly as possible and consider their job done if they change the policy 10 times a year to fit with changing practices within the company. However, there is a difference between informing consumers and respecting them. Managing privacy should not be seen by businesses as a burden. Instead, it can be a valuable way to generate and maintain a good relationship with your customers. Companies should view the establishment of a framework of consumer privacy controls as a key marketing and strategic variable that conveys considerable benefits.

Many large companies have privacy officers who set rules for managing data and audit compliance with those rules; however, hiring a privacy officer is usually seen by senior managers as a compliance cost. A company that respects the relationship with its customers, on the other hand, would think of the privacy officer as a strategic role and would establish a framework of consumer privacy controls as a key marketing and strategic variable.

This is not to say that compliance is irrelevant. Privacy regulations do exist, and all companies must abide by their legal obligations to their customers. However, the regulations that exist often provide little guidance to managers regarding how to manage consumer privacy. In the U.S., for example, a health-care law simply mandates that hospitals have a privacy policy, without making recommendations as to what it should be.

There are three strategies that companies can follow to transform touch points around privacy into a positive customer experience:

1. Develop user-centric privacy controls to give customers control.
2. Avoid multiple intrusions.
3. Prevent human intrusion by using automation wherever possible.

1. Develop user-centric privacy controls. Companies can make their customers feel helpless when it comes to their privacy. Privacy policies are usually drafted from a legally conservative perspective, from which a privacy policy that is vague or all-encompassing is seen as somehow benefiting the company if things go wrong. The result is lots of legalese that consumers either don't read or can barely understand. These policies are typically tucked away in remote corners of companies' websites, in companies' mailings to consumers and in responses to regulators. The result? While consumers often have no idea what companies' actual privacy practices are, our

research indicates that they have become more suspicious over time that companies are selling or misusing their data — even if companies are in fact managing consumer data appropriately. The legal department can insulate your company from legal risk, but not from consumer mistrust.

To address this issue effectively, companies should develop user-centric privacy controls that allow consumers to set limits on what aspects of their data the company can access. If consumers feel in control of their data, our research suggests that they become substantially more responsive to, for example, a targeted advertising message that relies on that data. Be up front about the types of data you are collecting about your consumers and with whom you are sharing it. For example, you could offer consumers a short menu of options when they register with your website or make a purchase through it. Use this process to drive registrations by specifying that registered users get more choice on how their data is used.

This conception of how to manage privacy goes beyond the overly simple notions of data privacy that have driven much of the political debate about online privacy. A lot of that discussion has focused on the notion of a global opt-in or opt-out through which consumers can choose to regulate companies' tracking of their movements online. However, the advertising-supported Internet would not exist today if consumers were in practice most comfortable with such an "all or nothing" approach. Actual online behavior more realistically suggests that consumers are sometimes more comfortable with companies tracking their behavior online and sometimes less. A major driver of their level of comfort is their level of perceived control over how their data is used. Consumers know best their own level of comfort with how companies use their data to improve their product offerings.

(Continued on page 12)

Why Managing Consumer Privacy Can Be an Opportunity (Continued from page 11)

The key for companies is to employ consumer-centric controls and to view them as an integral part of managing a positive customer relationship.

2. Avoid multiple types of privacy intrusion. At the heart of privacy is the ability to avoid unwanted intrusion. Technology has enabled multiple ways for companies to potentially intrude on consumers' privacy. Our research shows that intrusions backfire more in combination than separately.

For example, one way a company might intrude on its customer's privacy is by using web-browsing behavior to target relevant ads. Another is by physically trying to distract a customer's attention from the task at hand by, for example, using a pop-up ad. Our research shows that independently, consumers may accept either intrusion, but when companies intrude both ways at the same time — say, by using consumers' information to target them with unwanted, intrusive ads — such techniques backfire. This negative reaction seems to be related to an increase in awareness of the manipulative intent of the company. In other words, combining multiple privacy intrusions is particularly harmful to customer perceptions of the company.

Therefore, when using customer data to target messages, it is important to ensure that customers do not feel taken advantage of in another way. Ads that target web-browsing behavior will be most effective if they do not intrude too much on the computer screen; conversely, ads that pop up or take over a computer screen will be more effective if they do not also target prior web-browsing behavior. Similarly, automated telephone messages ("robocalls") will feel more intrusive if they start with a robotized voice addressing the consumer by name.

RELATED RESEARCH

- **A. Goldfarb and C. Tucker, "Online Display Advertising: Targeting and Obtrusiveness," Marketing Science 30, no. 3 (May-June 2011): 389-404.**
- **A. Goldfarb and C. Tucker, "Shifts in Privacy Concerns," American Economic Review Papers and Proceedings 102, no. 3 (May 2012): 349-353.**

3. Use automation to prevent human intrusion. Consumers are more comfortable when a machine processes their personal data than when a person does. For example, Google's Gmail serves ads on the basis of the text of people's emails. It is difficult to imagine that this would be accepted if a human were reading the emails. Human participation implies a personal judgment being made about the match between the customer and the ads served to him or her — and in that context, it is very easy to give offense. However, if ads are matched to customers purely via a computer algorithm, then a man receiving ads for "60% Off Mature Women's Swimwear" is more likely to be amused than offended.

Data security is different than a company's respect for its customers' privacy. Data security refers to a company's need to protect its consumers' privacy from external threats such as a malicious hacker. Privacy, on the other hand, refers to a company's need to protect its consumers from the company's own use of their data. Companies frequently focus on data security without recognizing that data may be accessed intrusively by their own employees. For example, the purchase history of a celebrity may be accessed by curious employees — and even if his or her purchases never make it into the press, this violates the celebrity's privacy.

Systems that can limit this kind of privacy violation are difficult to set up and maintain, however, because additional layers of internal security can interfere with the smooth running of a business and, in some circumstances, even with the quality of customer service provided. Reinforcing an informal culture in which privacy is respected and privacy violations are punished when they do occur may be a more workable and realistic solution than setting up elaborate formal systems that employees will find too cumbersome to use. The point here, as elsewhere, is less one of "data privacy" than "data courtesy" — treating customer data in a flexible and courteous way that allows consumers some power in the process.

Data collection and analysis are now cheap enough that anyone can collect vast amounts of customer data, and everyone is of sufficient commercial interest to have data collected on them. This data revolution has created opportunities for companies to provide customers with better-targeted products and services. We believe that managers who consider customers' reactions to the use of this data will have an advantage over their competitors. They will be better able to leverage the innovations enabled by customer data because their customers will welcome, rather than fear, these innovations.

However, this will only happen if companies shift from thinking about privacy as a compliance burden to thinking of treating data with courtesy as a fundamental part of the relationship with their customers. Privacy policies should be organized around managing customer data courteously, in accordance with consistent principles that customers feel comfortable with.

Avi Goldfarb *is a professor of marketing at the Rotman School of Management at the University of Toronto in Toronto, Ontario.* ***Catherine Tucker*** *is the Mark Hyman Jr. Career Development Professor and an associate professor of marketing at the MIT Sloan School of Management in Cambridge, Massachusetts. Comment on this article at http://sloanreview.mit.edu/x/54309, or contact the authors at smrfeedback@mit.edu.*

Reprint 54309.

MITSloan
Management Review

PDFs ■ Reprints ■ Permission to Copy ■ Back Issues

MIT Sloan Management Review articles, permissions, and back issues can be purchased on our Web site: *sloanreview.mit.edu* or you may order through our Business Service Center (9 a.m.-5 p.m. ET) at the phone numbers listed below. Paper reprints are available in quantities of 250 or more.

Customer Service
MIT Sloan Management Review
238 Main Street E48-570
Cambridge, MA 02142