Our perspective

The CMO's role in privacy

Are your marketing programs affecting your brand?

Customer data is one of your organization's most valuable assets. It yields insights into consumer preferences and purchase intentions. But even though the privacy issue surrounding such data is a hot topic among businesses and consumers, it has not traditionally been a priority among chief marketing officers (CMOs). That needs to change.

Given that 89% of consumers in a recent study say they avoid doing business with companies they think don't protect their privacy online,[1] CMOs should be concerned with the ways their customers' data is getting managed.

Do you know what your company's privacy policies are? Do you know who leads privacy aspects for your organization? Once, that area was the sole realm of the chief privacy officer (CPO) or the general counsel; now it's time for CMOs to take a more active role in managing and protecting customers' data.

The importance of trust

In seeking more-personal connections with customers, businesses collect and analyze customer data to better understand preferences and trends. The 2013 CMO Survey reported that 40% of companies use customer information collected online for targeting purposes and 88.5% of CMOs expect this practice to increase over time.[2]

However, with high-profile privacy violations occurring regularly, consumers are becoming more and more wary of sharing their personal information. If those consumers rebel and take steps to remove or mask their electronic footprints by means of techniques ranging from clearing cookies to browsing anonymously, to avoiding using loyalty cards, CMOs will be deprived of the information they need to effectively understand and target their audiences.

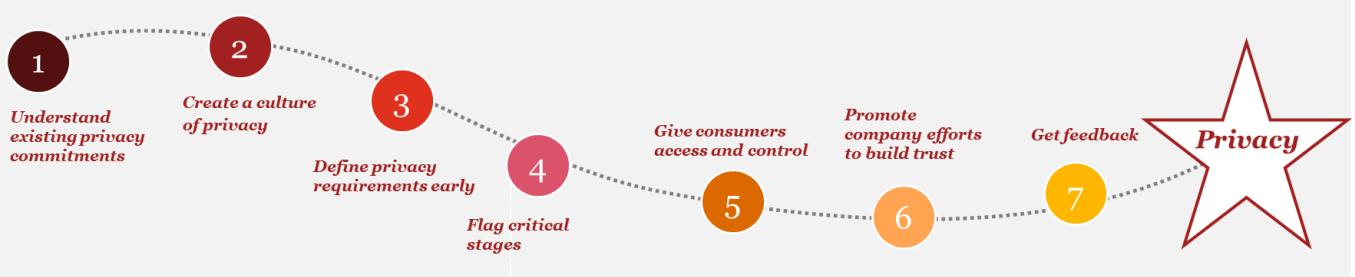
If you want consumers to provide complete and accurate information, they must trust you.

pwc

[1] 2014 TRUSTe US Consumer Confidence Index, http://www.truste.com/us-consumer-confidence-index-2014/.
[2] The CMO Survey, February 2014, http://www.cmosurvey.org/about/.

CMO privacy action plan

Here are some steps CMOs can take to protect consumer data and earn the trust of their customers.



1. **Understand existing privacy commitments.** Know the commitments already made to customers regarding how the organization will collect, store, share, and use personal information. Meet with your general counsel or CPO to discuss the company's customer-facing privacy policy and understand how it supports your marketing objectives. For organizations that have experienced mergers-and-acquisitions activity, data may have been collected under different commitments. In that situation, it may not be possible to treat collected data equally unless commitments and policies are harmonized and get communicated to customers. Finally, with more CMOs involved in global reaches, it's important to know the privacy laws of the countries targeted for marketing.
2. **Create a culture of privacy.** Champion the *thoughtful* use of personal information. Privacy should be embedded in the organization's objectives and marketing strategy, and CMOs should be vocal about those commitments. When working with teams—and especially vendors—include privacy on every agenda when discussing a marketing plan or creating new initiatives. Confirm that marketing agencies and any other subcontracted third parties are adhering to the company's privacy policies. Even if it's only a vendor—and not the company itself—that makes an error in the public eye, the matter will still come back to hurt your company's brand and trust.
3. **Define privacy requirements early.** Conceptualization is an important step in a new marketing initiative; it affects the overall design, requirements, and architecture of the final product. Influencing conceptualization is essential to integrating privacy concepts into product development and reducing the potential for the future misuse of data.
4. **Flag critical stages.** Establish checkpoints where disparate data sets get combined. These checkpoints help reduce the chance that sensitive information will be revealed. Businesses need to weigh the benefits resulting from data analytics with consumer privacy concerns—consider the customer's reaction if he/she were aware of how the data would be used.
5. **Give consumers access and control.** Your customers want to call the shots when it comes to their data. A recent PwC survey showed that 87% of customers want to be able to control the amount of information shared.[3] Make it easy for them to see what data you hold, and let them be the ones to determine how they want it used. The more comfortable they feel, the more they will trust you with their data.
6. **Promote company efforts to build trust.** View privacy as a marketing campaign in itself. Promote it. For example, highlight your company's responsible marketing policy. Consider taking it one step further by including it in the corporate sustainability report. In privacy marketing campaigns, it's important to articulate the value the consumer receives from your company's targeting initiatives, such as reduced spend or better product choices.
7. **Get feedback.** Open a channel for your consumers to provide feedback on marketing personalization. Was the personalization to their benefit or was it too intrusive? This is a great way to adjust future marketing campaigns based on the feedback received.

Make privacy a strategic plus

Today customers see value in an organization through its services, their purchasing experience, and product cost. In time, as the experience becomes more personalized, the privacy aspect will become one of the most important

[3] PwC, *Consumer privacy: What are consumers willing to share?* 2012, http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/consumer-privacy.jhtml.

ways to deliver additional value. CMOs should consider privacy not an obstacle to innovation and progress but, rather, another approach that builds customer loyalty levels.

Consider, create, and manage privacy activities as you would any strategically essential element of your organization. Make a necessity an asset.

Case in point

The following three case studies portray both the convergence of marketing and privacy activities and successful approaches to improving that interaction.

Integrated-media company

A large and integrated broadcasting, publishing, direct marketing, and digital media company had previously managed customer data separately within each of its discrete brands. With the arrival of a new senior-level data and marketing strategist, the company wanted to aggregate data across various brands. That data merge would yield sharper insights about customers and enable the company to cross-sell products and services.

The CPO quickly became aware of the challenges the new initiative would pose:

- Historically, privacy policies had been brand specific.
- Aggregation of customer data from varied sources could result in unpredictable privacy risks.
- The change might cause customer unease.

Accordingly, before launching the data aggregation pilot, the CPO and his advisors reviewed existing privacy policies and identified potential problem areas. The team then developed principles tailored to avoid the possible privacy risk exposures associated with cross-brand data integration.

Those actions enabled the company to embark on its big-data initiative safely—confident that privacy risks had been evaluated and would be managed effectively during the pilot. Moreover, the assessment served as a foundation for the future integration of individual-brand privacy policies into one single policy.

Large and integrated broadcasting, publishing, direct marketing, and digital media company

The chief financial officer and the general counsel wanted to better understand the privacy risks their organization faced as well as their organization's maturity and capabilities to appropriately mitigate and manage those risks. As a result of the assessment, senior management gained a better understanding not only of the company's existing privacy-related risks and capabilities but also of various company initiatives that collect, use, and/or share consumer personal data in new ways. Surprisingly, management learned that those company initiatives were likely missing out on opportunities to provide better user experiences or to further monetize data. This was due primarily to the conservative mind-set of the business as a result of lack of a privacy function that would advise on acceptable data collection, use, and sharing practices.

Prompted by the assessment's results, management began to strengthen its privacy program, which was cosponsored and directed by the chief strategy and marketing officer and the general counsel. Their charge included assigning responsibility for the privacy function and assembling a cross-functional privacy governance team that would develop measures for remediation and governance of the evolving privacy risks and that would help enable the business to use customer data more effectively.

As a result of those executive actions as well as the clear governance structures put in place for using customer data, the company is on its way to the confident use of customer data that will improve the customer experience and grow top-line revenue while continuing to protect privacy and maintain trust and transparency with customers.

Large global retailer

For this company, digital marketing was a major focus. Management wanted confirmation that customers' privacy rights were being honored and that the company's privacy policy was being enforced. The greatest risks were seen in customer outreach emails and text messages, along with data management and sharing practices with key third parties.

An assessment of privacy and data protection risks focused on:

- The alignment of customer relationship management (CRM) activities with the company's privacy policy
- The customer data management process: acquisition, storage, use, sharing, archiving, and disposal

Post assessment, the company established the main steps that CRM personnel were required to follow in outreach programs involving customers' personal information. In addition, use cases were developed that (1) described the operational context in which the steps would come into play, (2) identified the stakeholders likely to be affected, and (3) highlighted related business decisions.

Through those measures, the digital marketing team was able to inform management that privacy and data protection requirements were being applied consistently and were repeatable for both current and new team members.

Contacts

For an in-depth discussion of the challenges your organization faces at the intersection of marketing and privacy, please contact:

Carolyn Holcomb
Cybersecurity and Privacy
Partner
PwC
(678) 419-1696
carolyn.c.holcomb@us.pwc.com

Jay Cline
Cybersecurity and Privacy
Principal
PwC
(612) 596-6403
jay.cline@us.pwc.com

Joe Divito
Cybersecurity and Privacy
Principal
PwC
(412) 355-8067
joseph.v.divito@us.pwc.com

Gary Loveland
Cybersecurity and Privacy
Partner
PwC
(949) 437-5380
gary.loveland@us.pwc.com

Mark Lobel
Cybersecurity and Privacy
Principal
PwC
(646) 471-5731
mark.a.lobel@us.pwc.com