

Project Type: Research Report

Details: Developed a 26-page research report (including appendix) that detailed the findings of a study from the Ponemon Institute highlighting possibly privacy concerns that arise as a result of marketing activities.

Excerpt:

Are U.S. marketers and privacy and data protection practitioners miles apart in their beliefs about how their organizations should and do protect consumers' information in email marketing campaigns? If so, does such a gap in their beliefs indicate that organizations are putting personal information at risk?

The study entitled *2008 U.S. Study on Email Marketing Practices & Privacy* was conducted by Ponemon Institute and sponsored by StrongMail. The findings reveal gaps in perceptions between marketers and privacy professionals about how email marketing practices affect consumers' privacy rights and risks to personal information. While both groups believe that it is important for consumers and customers to trust the privacy commitments of organizations, marketers worry that complying with privacy regulations could hinder their ability to attract new customers. This ability is core to their role in their organizations and is how their success is measured. The role of the privacy professional is to focus on compliance with regulations and to ensure that steps are taken to secure personal data.

According to the study, more than one-third of marketers do not limit the data they distribute to third parties, whereas 75% of privacy professionals believe that their organizations limit the data it shares. Marketers will share such personal information as credit card number (45%), debit card number (39%), Social Security number (29%), and bank account/routing number (17%).

Further, there is the tendency to outsource marketing campaigns to third parties. Fifty-nine percent of marketers and 53% of privacy professionals indicate that their organizations outsource to reduce costs and improve efficiency. However, our study finds that almost half of the organizations that experienced a data breach pinpointed the loss of data to a third party, such as a vendor, business partner or contractor.

