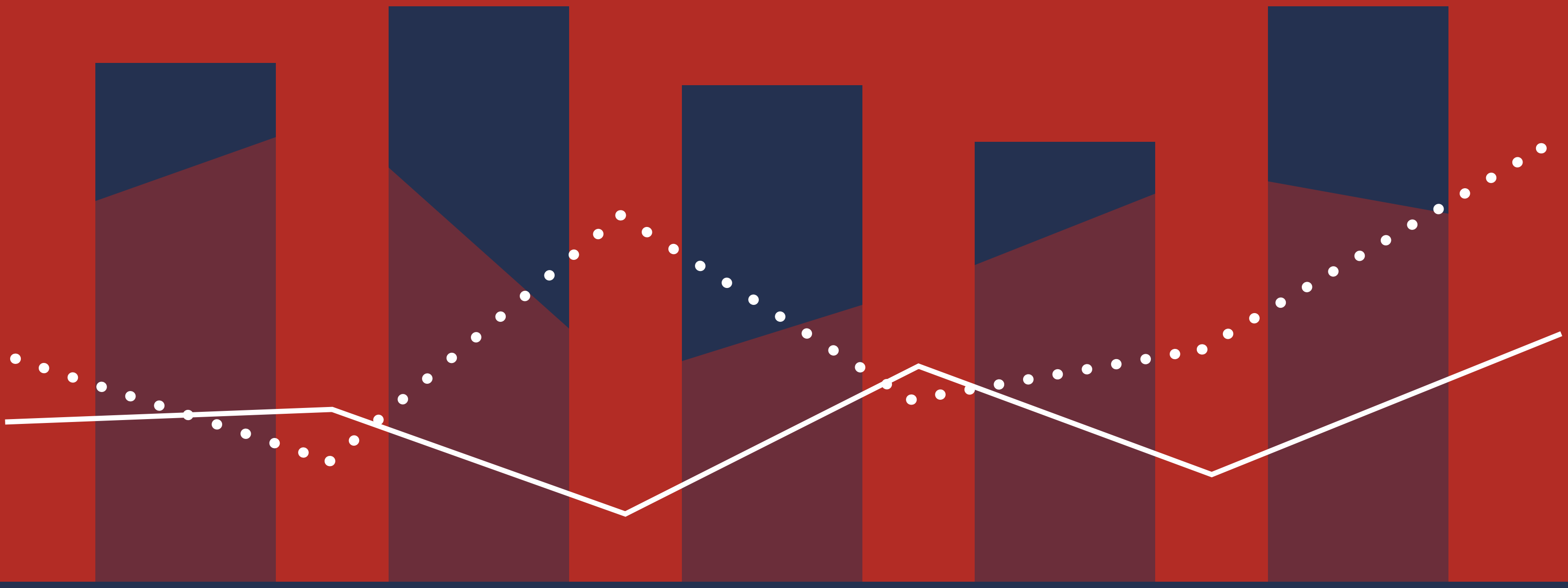
IMPACT AT JMR

JOURNAL *of* MARKETING RESEARCH



AMERICAN MARKETING ASSOCIATION

The Marketer at the Privacy Table

Sachin Gupta, Panos Moutafis and Matthew J. Schneider | 3.17.2022

Many executives and corporate administrators believe their marketing department should have a limited role when it comes to customer privacy. They believe the department should only manage customers' privacy perceptions. Actual data security decisions should be left to the information technology department, and privacy decisions should be made by legal.

However, marketing professionals bring practical knowledge and techniques to the data privacy discussion that can effectively limit the consumer information collected without impacting its usefulness.

The Exclusion Error

Excluding marketers from data gathering decisions can result in firms collecting too much information and increasing customer exposure risks. Consider the 2020 data breach at insurance software provider Vertafore. The information leak included license numbers, names, addresses, birthdates, and vehicle registration histories of about 27.7 million drivers in Texas. Had marketers been at the decision table from the beginning, Vertafore may have known that its insurance company clients did not need drivers' personal details to model risk and premiums.

Marketers can also provide firms valuable insights for decisions about protecting privacy after data have been gathered. For example, ACNielsen averages retail sales and prices across stores within markets, California legislators require household energy usage data to be grouped by at least 15 households, and Google aggregates its sponsored search data at the daily level—all partly for privacy reasons. But the aggregation can result in biased marketing activity estimates (Christen et al. 1997) and limit the companies' targeting capabilities.

Perception Good, Protection Better

Marketing researchers have offered insights into the effects of improved perceptions of privacy as well as ways to strengthen privacy protection (Table 1). They find that when firms improve perceptions of privacy, consumers express greater willingness to share data, trust their brand, and respond to marketing activities. To improve protection, firms can alter their data processing protocols to increase privacy while preserving insights. Marketing professionals can apply the techniques during data gathering, after data gathering, or both.

Table 1: Selected marketing-focused data privacy research

Goal	*After Data Gathering*	*During Data Gathering*
Perception	**1** Tucker 2014; Martin, Borah, and Palmatier 2018	**2** De Jong, Fox, and Steenkamp 2015
Protection	**3** Zhou, Lu, and Ding 2020; Schneider et al. 2018	**4** De Jong, Fox, and Steenkamp 2015; Gupta, Moutafis, and Schneider 2021

Tucker (2014) found that Facebook users were nearly twice as likely to react positively to personalized advertising after the platform gave them increased control over their personal information (i.e., enhanced perceived privacy). Martin, Borah, and Palmatier (2018) found that firms providing customers data transparency and control were not punished as severely upon breach as were less transparent firms.

Extensive literature (e.g., De Jong, Fox, and Steenkamp 2015) has offered randomized survey response techniques to elicit truthful answers, especially to sensitive questions. The methods influence respondents' beliefs about the privacy of their own answers and increase data protection. Other research has explored approaches to alter data statistically after collection to reduce the likelihood of disclosing personal information while preserving insights. Applications include facial images (Zhou, Lu, and Ding 2020) and point-of-sale data (Schneider et al. 2018).

Finally, Gupta, Moutafis, and Schneider (2021) highlight the privacy benefits of edge computing, whereby firms do not transmit or retain sensitive information, minimizing data risks.

A Theoretical Take

Firms often alter customer data to increase privacy. Theorists consider "differential privacy" the gold standard. Analysts create differentially private data by introducing inaccuracies to limit the likelihood of disclosing an individual's identity. But currently available differential privacy approaches can result in useless data for many practical marketing applications.

A new set of methods, such as shuffling algorithms and generative adversarial networks, allow data protectors to model marketers' information needs explicitly in the protection process. Specifically, the models' loss function embodies the desired insights and ensures that the randomly generated synthetic data do not lack valuable information. Schneider et al. (2018) demonstrate how analysts can preserve estimated price and promotion elasticity precision in a market response model applied to point-of-sale data. Zhou, Lu, and Ding (2020) show how firms can preserve useful consumer facial cues while transforming full facial images into contours.

Summary

Firms must consider how their marketers will use data before they set their privacy policy to maximize the data's usefulness. And marketing effectiveness estimates are less biased when firms tailor their data protection to their marketers' needs.

Brands benefit from improved customer privacy perceptions, and many make an intrinsic promise that their customers' data are private. However, customers must not only perceive that their data are safe; their data must actually be safe.

Marketing scholars and practitioners must therefore focus on helping firms protect their data without limiting usefulness.

Rather than be excluded from the privacy table, marketers should spearhead data protection and privacy efforts. Marketers not responsible for data protection might collect too much information, and data privacy decisions made without marketing might compromise valuable insights. Furthermore, marketers make their firms' privacy promises to consumers and manage public relations after data breaches. Therefore, they are intrinsically motivated to uphold the brand promise.

AUTHORS

Sachin Gupta is the Henrietta Johnson Louis Professor of Management and Professor of Marketing at the SC Johnson College of Business at Cornell University, Ithaca, New York, and Editor-in-Chief of the Journal of Marketing Research.

Panos Moutafis is a Computer Science Ph.D. and co-founder and CEO of Zenus, a startup specializing in ethical artificial intelligence and computing solutions.

Matthew J. Schneider is an Assistant Professor of Statistics and Data Privacy at the LeBow College of Business at Drexel University, Philadelphia, Pennsylvania.

CITATION

Gupta, Sachin, Panos Moutafis, and Matthew J. Schneider (2022), "The Marketer at the Privacy Table," Impact at JMR, (March), Available at: https://www.ama.org/2022/03/17/the-marketer-at-the-privacy-table/

REFERENCES

Christen, Markus, Sachin Gupta, John C. Porter, Richard Staelin, and Dick R. Wittink (1997), "Using Market-Level Data to Understand Promotion Effects in a Nonlinear Model," Journal of Marketing Research, 34 (3): 322–34. https://doi.org/10.2307/3151895

De Jong, Martijn G., Jean-Paul Fox, and Jan-Benedict E.M. Steenkamp (2015), "Quantifying Under- and Overreporting in Surveys through a Dual-Questioning-Technique Design," Journal of Marketing Research, 52 (6): 737–53. https://doi.org/10.1509/jmr.12.0336

Gupta, Sachin, Panos Moutafis, and Matthew J. Schneider (2021), "To Protect Consumer Data, Don't Do Everything on the Cloud," Harvard Business Review, June 29, 2021. https://hbr.org/2021/06/to-protect-consumer-data-dont-do-everything-on-the-cloud

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier (2018), “Research: A Strong Privacy Policy Can Save Your Company Millions,” Harvard Business Review, February 15, 2018. https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions

Schneider, Matthew J., Sharan Jagpal, Sachin Gupta, Shaobo Li, and Yan Yu (2018), “A Flexible Method for Protecting Marketing Data: An Application to Point-of-Sale Data,” Marketing Science, 37 (1): 153–71. https://doi.org/10.1287/mksc.2017.1064

Tucker, Catherine E. (2014), “Social Networks, Personalized Advertising, and Privacy Controls,” Journal of Marketing Research, 51 (5): 546–62. https://doi.org/10.1509/jmr.10.0355

Zhou, Yinghui, Shasha Lu, and Min Ding (2020), “Contour-as-Face Framework: A Method to Preserve Privacy and Perception,” Journal of Marketing Research, 57 (4): 617–39. https://doi.org/10.1177/0022243720920256

About JMR

The *Journal of Marketing Research* delves into the latest thinking in marketing research concepts, methods and applications from a broad range of scholars. It is included in both the *Financial Times* top 50 business journals and the University of Texas Dallas research rankings journal list.

About Impact at JMR

Impact at JMR highlights important and actionable content published in the *Journal of Marketing Research*. Executives can leverage this content in their organization. Professors can use it in their classrooms. Researchers can learn about distinct scholarly insights for their next big idea. We invite everyone to read, enjoy, learn, think and act.