The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://sloanreview.mit.edu/article/why-managing-consumer-privacy-can-be-an-opportunity/">http://sloanreview.mit.edu/article/why-managing-consumer-privacy-can-be-an-opportunity/</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>MIT Press</td>
</tr>
<tr>
<td>Version</td>
<td>Original manuscript</td>
</tr>
<tr>
<td>Accessed</td>
<td>Sun Feb 03 17:02:07 EST 2019</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/88197">http://hdl.handle.net/1721.1/88197</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Creative Commons Attribution-Noncommercial-Share Alike</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td><a href="http://creativecommons.org/licenses/by-nc-sa/4.0/">http://creativecommons.org/licenses/by-nc-sa/4.0/</a></td>
</tr>
</tbody>
</table>
MANAGING PRIVACY

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? Firms 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 ten times a year to fit with changing practices within the firm. We want to draw a distinction between informing your consumers and respecting your consumers. Managing privacy is not a burden. It is a valuable way to generate and maintain a valuable relationship with your consumers.

Ensuring consumer privacy is often seen as a burden. While many companies have privacy officers, these are not strategic roles. Instead, privacy officers typically set and audit rules, and their actions are seen as a cost for compliance. In this article we argue that firms should stop viewing the protection of their consumer’s privacy as simply about compliance. Instead we encourage firms to view the establishment of a framework of consumer privacy controls as a key marketing and strategic variable that itself conveys considerable benefits.

There are many ways that firms can think about privacy as being a matter of informing rather than respecting consumers. Many large firms have privacy officers who set rules for managing data and audit compliance with those rules; hiring a privacy officer is seen by senior managers as a compliance cost. A firm that respects the relationship with its consumers, 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 that itself conveys considerable benefits to the firm. None of this is to say that compliance is irrelevant. Privacy regulations do exist, and all firms must abide by their legal obligations to their customers. However, the regulations that exist provide little guidance to managers regarding how to manage consumer privacy. In the healthcare field, for example, in many cases HIPAA mandates simply that hospitals have a privacy policy, without making recommendations as to what it should be. So, this article is about what else you should or should not do after you have met your legal obligations.

We describe three general touchpoints where consumers have privacy concerns in the way that the firms interact with them. We describe strategies that all firms should follow to transform these touchpoints into positive customer experiences. These touchpoints are:

1. Lack of Control
2. Multiple Intrusions
3. Human Intrusion

We consider three potential policies that can help mitigate these concerns for companies with a thoughtful approach to consumer privacy protection.

Avi Goldfarb is Professor of Marketing, Rotman School of Management, University of Toronto, 105 St George St., Toronto, ON. Tel. 416-946-8604. Email: agoldfarb@rotman.utoronto.ca. Catherine Tucker is Associate Professor of Marketing, MIT Sloan School of Management, 100 Main St, E52-533, Cambridge, MA. Tel.617-253-1499. Email: cetucker@mit.edu.
(1) Enabling User-Centric Privacy Controls → Mitigation of risk of customer reactance.\(^1\)
(2) Avoiding multiple layers of privacy intrusion → Mitigation of risk of customer perception of manipulative intent.
(3) Ensuring security through automation → Mitigation of customer concerns of being judged by others.

1. USER-CENTRIC PRIVACY CONTROLS

Firms often make their customers feel helpless when it comes to their privacy. This often happens by accident. The people who draft a firm’s privacy policies are often approaching privacy from a legally conservative perspective, where a privacy policy that is vague or all-encompassing may somehow benefit the firm if things go wrong. The result is screeds of legalese that consumers don’t read, or hardly understand if they do read them. The screeds can be found in remote corners of firms’ websites, in firms’ mailings to consumers, and in responses to regulators. The result with respect to consumers is that consumers have no idea what firms’ actual privacy practices are, but become more suspicious over time that firms are probably selling or misusing their data even if firms are in fact managing consumer data appropriately. The legal department can insulate your firm from legal risk, but not from falling sales caused by increased consumer reactance.

To address this issue effectively, one step firms can take is to empower their consumers to manage their own privacy. To do so, they need to develop a set of user-centric privacy controls which allow consumers to set limits on what aspects of their data the firm can access. If consumers feel in control of their data, our research shows that they become substantially more responsive to targeted advertising messages that rely on data about consumers. How this can work in practice is to be up front about the types of data you are collecting about your consumers and whom you are sharing it with. You could, for example, offer consumers a short menu of options when they register with your website or make a purchase through it. You can use this process to drive registrations by specifying that registered users get to choose how their data is used.

This conception of how to manage privacy goes beyond the overly simple notions of data privacy that have driven the political debates about privacy in government. A lot of discussion has focused around the notion of a global opt-in or opt-out of firms tracking your movements online. However, the advertising-supported internet would not exist today if consumers were in practice most comfortable with an “all or nothing” approach. Consumers’ actual behavior online more realistically suggests that they are sometimes more comfortable with firms tracking their behavior online and sometimes less, with a major driver of their level of comfort being their level of perceived control over how their data is used. Consumers know what data they feel comfortable with a firm using to improve its communications with and treatment of them. The key for firms is to employ consumer-centric controls and view them as an integral part of managing a positive customer relationship.

\(^1\)‘Reactance’ is a psychological term for a negative response to instances when firms take freedom away from their consumers. Reactance is harmful for a firm because it sets consumers into a mindset where they are likely to view engagements with the firm as confrontational. In the privacy context, it is partially a response to increased awareness of manipulative intent. Every mailing a firm sends to consumers regarding a change to privacy policies has the potential to increase reactance and damage the relationship with your consumers.
2. AVOIDING MULTIPLE LAYERS OF PRIVACY INTRUSION

Privacy is a term that covers many conceptually distinct ideas. One way a firm may intrude on its customer’s privacy is by using web browsing behavior to target relevant pharmaceutical ads. Another way is by physically trying to distract a customer’s attention from the task in hand. Our research shows that customers value both of these aspects of privacy, but that it is when firms use information to target customers with unwanted intrusions that customers react strongly. Our research suggests this relates 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 some other dimension. Ads that use web browsing behavior will be most effective if they are designed to not intrude much physically on the computer screen; conversely, ads that pop up or take over a computer screen will be most effective if they do not also target using prior web browsing behavior.

3. PREVENTING HUMAN INTRUSION

Consumers are more comfortable when a machine processes their personal data than when a human processes the same data. To take an illustrative example, gmail.com serves ads on the basis of the text of people’s emails. It is difficult to imagine that this system could have won acceptance 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 that customer, 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 Swimwear” is more likely to be amused than offended.

Data security and a firm’s respect for its customers’ privacy are conceptually distinct. Data security refers to a firm’s need to protect its consumers’ privacy from external threats such as a malicious hacker. Privacy refers to a firm’s need to protect its consumers from the firm’s own use of their data. Too often firms focus on preventing consumer data from being seen by humans outside of their walls, without recognizing that data being seen by its own employees may also be intrusive. In the field of medical records, for example, it is common for celebrities’ records to be accessed from within the hospital by curious employees, and this violates their privacy even if their medical records never make it into the press. Systems that can limit this kind of privacy violation are difficult to set up and maintain, because additional layers of internal security automatically inconvenience the smooth running of a hospital and may, in certain circumstances, even threaten the quality of care provided (Miller and Tucker 2009). Firms may therefore find it more advantageous to work on reinforcing an informal culture where privacy will be respected and punishing privacy violations when they do occur, rather than setting up over-elaborate formal systems that employees will then find too cumbersome to use. The point here, as elsewhere, is less one of “data privacy” than “data courtesy” - limiting customer reactance by treating their data in a flexible and courteous way that allows customers some power in the process.

4. CONCLUSION

It used to be the case that privacy concerns only affected a firm’s most prominent customers. Now, data collection and analysis are cheap enough that anyone can collect vast amounts of customer data and everyone is of sufficient commercial interest to have data collected on them.
It is well-established that this data has created opportunities for companies to provide customers with better-targeted products and services. In this article, we argue that managers who consider the potential for reactance to usage 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, innovations made with their data.

However, this will only happen if firms shift conceptually from thinking about the “burden of privacy” 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.

5. SOURCES


ABOUT THE AUTHORS

Avi Goldfarb is Professor of Marketing in the Rotman School of Management at the University of Toronto. He received his PhD in economics from Northwestern University. His research examines the impact of information technology on marketing, on universities, and on the economy.

Catherine Tucker is the Mark Hyman, Jr. Career Development Professor and Associate Professor of Management Science at MIT Sloan School of Management. She is interested in understanding how networks, privacy concerns and regulation affect marketing outcomes. She received an undergraduate degree in Politics, Philosophy and Economics from Oxford University and a Ph.D. in Economics from Stanford University.