MIT Sloan Management Review

SPECIAL COLLECTION

FALL 2017

CUSTOMER SERVICE

The Fine Line Between Service and Privacy

How to balance service with security in digital business.

CONTENTS

SPECIAL COLLECTION
FALL 2017

The Fine Line Between Service and Privacy

[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.

Improving Customer Service and Security With Data Analytics

The advantages of analytics to customer service have already been shown. Now the question becomes: How can analytics be used to improve security?

BY SAM RANSBOTHAM

ORGANIZATIONS are collecting more and more data. And while rich data allows personalized service, detailed data about real people (rightly) often raises concerns. Just as this data is increasingly valuable to organizations, it can be valuable to criminals as well, leading to an ever-escalating series of data breaches. Data analytics exacerbates trade-offs between security and service; the analytical processes on data can, at a minimum, raise privacy concerns for individuals because much of marketing analytics tries to learn as much as possible about potential customers. These analytics processes are becoming increasingly powerful at de-anonymizing people from their trace data.

However, these de-anonymization techniques are an example of a way that analytics offers at least a partial solution to the problems it has exacerbated.

Consider, for example, placing a call to your bank for help after losing your debit card. The core problem is that, before providing customer service, the bank must authenticate that you are who you say you are. This authentication process must begin with the assumption that the caller is a malefactor impersonating the real customer — guilty until proven innocent. The bank will help the caller *only* after being convinced of the caller's identity.

While this process is annoying when we're customers seeking help, we actually want and need this level of security. It is in our best interests that the bank will verify that we are who we say we are before continuing to assist us. After all, we don't want the bank to hand out our money (or our new debit card) willy-nilly to just anyone.

Historically, this telephone authentication process involves answering a set of questions. What is your account number? What is your personal identification number (PIN)? What is your Social Security number? Can you verify the last three transactions in the account? What is your prior address? The process continues, potentially escalating to security challenge questions based on shared secrets, until the bank is convinced of our identity.

This process is adversarial by design. Even the name "security challenge question" evokes a combative stance, a challenge. The initiator of the call is not trusted until passing through a gauntlet. For banks, it is unfortunate that so many initial interactions with a customer are adversarial in nature.

But data and machine learning, specifically speech processing, offer a great example of an invisible way that analytics can simultaneously help improve security and service. The technology itself isn't that new, but speech processing has progressed to the point now where financial services companies can match a caller's voice to their prior calls, allowing the authentication process to occur behind the scenes as the customer service conversation progresses.

Fidelity Investments, for example, encourages the use of voiceprints to confirm identity within the first moments of a conversation. HSBC is beginning to do this not just for premier clients, but at scale for retail clients as well. And the change doesn't just help the customers avoid yet another password or secret question: Barclays notes a 20-second reduction in time to authenticate — and those 20 seconds add up quickly to considerable savings in employee time for the bank.

The convenience and savings may be the initial drivers of this change. However, perhaps a bigger effect, more elusive to quantify, is the change in orientation. Data and machine learning can ensure that the customer interaction begins by focusing on assistance rather than challenge. Customer service can work with, not against, a caller who (in all statistical likelihood) is a genuine customer, not a con artist — innocent until proven guilty, in other words. Customer service doesn't have to assume initially that callers *might* be nefarious — and identity validation can occur in parallel while the conversation is getting started. This means that the unlikely (but potentially damaging) scenario that a security threat exists doesn't have to poison the majority of interactions with valid customers — without leaving it unaddressed. Organizations can relegate the pesky security issues to behind the scenes, where they should be kept. The authentication process is passive, churning along in the background. Security must only become visible if a problem is found. In this case, the artificial intelligence is augmenting the human employee in ways that are not visible to the customers.

As a result, valuable and expensive training time for customer service employees can be spent more on banking and less on security. While the direct result is more effective customer-service training, the indirect result is scale. When a new security threat emerges, the bank can deploy countermeasures quickly to all customer service interactions.

And more can likely come from this initial application. For example, a customer may in fact be who they say they are, but may be being coerced. Or they may be suffering from some impairment. Speech patterns that indicate these possibilities can be brought to the attention of the customer service agent for further assessment.

Because it is, by definition, an invisible process, examples like this may get far less attention than humanoid robots or chatbots. But analytics can help mitigate some of the trade-offs between the security and service that increased data collection exacerbates. These applications may have a far greater effect on customer relationships for organizations than the ostentatious examples that may be more effective at marketing than managing.

Sam Ransbotham *is an associate professor of information systems at the Carroll School of Management at Boston College and the* MIT Sloan Management Review *guest editor for the Data and Analytics Big Ideas Initiative. He can be reached at sam.ransbotham@bc.edu and on Twitter @ransbotham.*

[RISK MANAGEMENT]

What Executives Get Wrong About Cybersecurity

If you think the biggest cybersecurity threat most businesses face is credit card theft and the most important part of the solution is better prevention technology, think again.

STUART E. MADNICK, INTERVIEWED BY MARTHA E. MANGELSDORF

Cyberattacks are in the news. All kinds of organizations — ranging from Target Corp., Yahoo Inc., Sony Pictures Entertainment, and Bangladesh Bank to the Democratic National Committee in the United States — have fallen victim to them in recent years. To gain a better understanding of cybersecurity threats — and what executives should do to better protect their companies — *MIT Sloan Management Review* sought out cybersecurity expert Stuart E. Madnick.

Madnick has been studying computer security for a long time. He coauthored his first book on the subject in 1979 and today is the director of MIT's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³, a consortium that brings together academic researchers, companies, and government experts. Madnick, who is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management and a professor of engineering systems at the MIT School of Engineering, spoke about trends in cybersecurity recently with *MIT Sloan Management Review* editorial director Martha E. Mangelsdorf. What follows is an edited and condensed version of their conversation.

***MIT SLOAN MANAGEMENT REVIEW:* Why did the MIT cybersecurity consortium you lead choose to focus on the nation's critical infrastructure?**

MADNICK: Much of the attention about cybersecurity has been focused on things like stealing credit cards — which is important, and we don't neglect that. But surprisingly little attention has been paid to cyberattacks on critical infrastructure. You don't hear much about the Turkish pipeline explosion or the German steel mill meltdown. You may have heard a little bit about the cyberattack on the Ukrainian power grid that happened around Christmas in 2015. Generally, these events involving attacks on infrastructure do not get much attention; they're not quite as sexy as movie stars' emails being revealed. But they have the potential to have far bigger impact.

Our feeling is that we need to increase the attention we pay to cybersecurity for important infrastructure. It doesn't mean we're going to ignore everything else, but there are some things that are particularly unique to those kind of attacks.

Think about preparedness. For example, what if it turns out that a cyberattack causes the New England power grid to go down — and remain down — for three months? What preparation has the governor of Massachusetts, the mayor of Boston, or MIT made for going three months without power? The answer is probably "not enough."

Losing power for such a long time is not out of the question. How is this possible? If your personal computer goes dark, what do you

do? You reboot it. If worse comes to worst, you wipe it clean and reload it. But imagine if your turbine breaks down due to a cyberattack. You can't just go to a local turbine store. For example, MIT's cogeneration facility had a turbine failure recently — not because of a cyberattack, but because of mechanical failure due to a simple defective nozzle. Still, it took three months to repair the turbine; these things are huge, and many of the parts aren't readily available.

Let me tell you about the attack on the Ukraine power grid in 2015, because it's a fascinating story. The Ukraine is divided into a number of separate power grids, much like the U.S. Three of the power grids were attacked and went down, and about 225,000 people lost power for several hours.

I attended a briefing about the attack; there were a number of people, particularly from the U.S., who went over to Ukraine to understand exactly what happened. And I was surprised by two of the investigators' conclusions.

The first conclusion had two parts:

1. The attack was low in sophistication. The attackers used seven different techniques to down the grid, but all of them were readily available for sale on the internet. No new weapon had to be created; there is a huge cybercrime ecosystem operating on the internet.
2. But the attack was high in organization. The hackers had to go and assemble the seven weapons together. And they did some very clever things. Not only did they down the power grid, they also shut down the backup system, so even the power company had difficulty getting back online. They also erased all the disks, so it was hard to track down what they had done.

And then to add insult to injury, they overloaded the power company's call center so that customers couldn't call in to tell the power company that they lost power. How is that for being malicious? This was not a teenager doing a casual hack.

The second conclusion that investigators came to as they looked into the attack was: This was only a demonstration. The hackers could have done much, much more damage. This was a political statement, saying in effect: "We're here. We're not going away." And, in this case, the finger is pointing to the Russians.

But we can't be sure about that. I met someone who does hacking for governments. He happens not to work for the U.S., Russia, or China. He says that, in all of the software he and his colleagues develop, they make sure that all of their comments are in Chinese. The point being: If you're really good at hacking, you'll make sure all the evidence points to someone else. So if you think you know who is behind a hacking attack, most likely that isn't who it is.

"If you don't address the managerial, organizational, and strategic aspects of cybersecurity, you're missing the most important parts."

— STUART E. MADNICK

What are the most important things business executives can do to decrease their companies' cybersecurity vulnerabilities?

MADNICK: If you don't address the managerial, organizational, and strategic aspects of cybersecurity, you're missing the most important parts. A lot of people are working on developing better hardware and software, and that's good. That's important. But that's only a piece of the puzzle.

Estimates are that between 50% and 80% of all cyberattacks are aided or abetted by insiders, usually unintentionally — typically through some kind of "phishing" expedition [involving emails containing a link or attachment to click on]. Untargeted mass phishing emails have an open rate of 1% to 3%. But highly targeted "spear phishing" is much more effective, with an open rate of about 70%. With spear phishing, you'd get an email that appeared to come from a high-ranking executive at your company, that referred to you personally and that asked you to take some specific action consistent with your job, such as authorizing a new employee or transferring funds to a new vendor.

So if you don't address the people issues, you're missing the really hard cybersecurity problems. A lot of the vulnerabilities that exist in organizations come from the corporate culture we create and the practices we have. I'll give you some examples.

We work with energy companies. I was talking to someone who had visited the headquarters of one of them, and he said that if you're going up or down the stairs and not holding the railing, someone will actually stop you and say, "Please hold the railing, for safety." That's how ingrained they have gotten the idea of safety. I was told that if you're walking down the hallway texting on your phone, someone will say, "Stop. Either do your texting, or do your walking. Don't do both." Because they understand that if they do something wrong in oil refining, plants can blow up, and people die. That safety mindset permeates the organization.

Another example is: When you walk into an industrial plant, you will often see a sign that says, "520 days since the last industrial accident." If you walk into a data center, do you ever see a sign that reads, "520 milliseconds since the last successful cyberattack?" Do you even know how many attempted cyberattacks there are on your company on a typical day?

Companies need to develop that kind of safety culture and mindset about cybersecurity. Think of it this way: I could put a stronger lock on my door, but if I'm still leaving the key under the mat, have I really

What Executives Get Wrong About Cybersecurity
(Continued from page 23)

made things any more secure? Although that's an oversimplification, that's the phenomenon in organizations: We're building stronger doors but leaving keys all over the place. That's why the organizational and managerial aspects of cybersecurity are so critical.

But cybersecurity has to be done across the value chain, doesn't it? Because it's not enough if your company has great cybersecurity policies, if they don't extend to your suppliers.

MADNICK: You're right. People often use the expression "e2e" — end to end. Your piece of the puzzle may be perfectly secure, but nowadays, everybody is interconnected in one way or another.

For example, the break-in that Target experienced took place through a heating, ventilation, and air conditioning maintenance company, which had access to some Target systems. Likewise, the SWIFT messaging platform for financial institutions was exploited through vulnerabilities at Bangladesh Bank, which lost $63 million.

Is there any industry that you see doing a really good job at managing cybersecurity issues?

MADNICK: I'd rate industries from poor to terrible. On that scale, financial services is probably doing a better job than most other industries. On the other hand, they're the ones who are probably the targets of the largest number of attacks. So they may be twice as good at cybersecurity, but if they have four times as many attacks, that doesn't mean they're in great shape.

I don't know which industry is the poorest, but hospitals clearly are vying for that position. According to one recent report, 88% of all detected ransomware attacks [where computers are "held hostage" unless the user pays] on organizations are targeted to hospitals, because they're easy targets. If you're a hospital and you're held up for ransomware, would you pay it or not? If your hospital's computers are held hostage, the patients in the hospital are now to some extent at increased risk. You no longer have access to up-to-date medical records, such as test results and changes to medication. So by not paying, you are possibly putting people's lives at risk.

What cybersecurity advice would you like to give to *MIT SMR*'s audience of business executives?

MADNICK: Think in terms of a three-pronged approach: prevention, discovery, and recovery. Gartner recently came out with a report entitled "Prevention Is Futile in 2020." This is consistent with our viewpoint that if the Pentagon can be broken into, if the NSA [U.S. National Security Agency] can be broken into, if the Israeli Defense Forces can be broken into, why do you think you can't be broken into?

That's why you need to think in terms of all three steps. Of course, you want to do as much prevention as you possibly can, within reason. But the next two steps are detection and recovery. According to several studies, the average cyberintrusion can go on for more than 200 days before it is discovered. I also read a recent report that says in the Asia Pacific region it's 520 days — more than double.

So our ability to detect that something funny is going on is pretty poor. By the time you discover the attack, the hackers have probably been rummaging around, stealing documents, and doing things for a long time.

I joke that if at 5 o'clock every day, one of the people leaving the bank walks out with a wheelbarrow full of money, do you think someone would notice after a few days? Yes, probably! But things like that happen all the time in computer systems, and nobody is paying attention. Maybe it's not quite as visual, but there are funny things going on, and often no one is even looking to see if there's anything suspicious.

And then finally, recovery is very happenstance. By and large, CEOs are caught unprepared when someone shoves a microphone in front of them to talk about the cyberattack that was just discovered at their company. And that's just part of the recovery. Other questions to figure out: Have we actually cleansed our system, or is the attack still going on? How do we make sure it doesn't happen again next week?

Much like my comment that industries range from poor to terrible on cybersecurity, the same thing applies to the three prongs. Most organizations are poor at prevention, pretty bad at detection — and probably terrible at recovery.

I jokingly say that not that long ago, cybersecurity was a task you assigned to the junior assistant programmer trainee, and his job was to go desktop to desktop loading the latest Microsoft patches. Now you're having the CEO of the company being interviewed by the news station when a cyberattack is discovered. So it's been a total inversion, if you will, up to the highest level of the organization. Until recently, most CEOs barely even knew how to spell cybersecurity! So there are lots of issues to deal with. What is the cybersecurity education needed at each level of the organization? What is the preparation needed? How do we deal with these attacks? Executives need to take these questions seriously.

Back in 1979, I coauthored a book called *Computer Security*. What's interesting is that the conclusion to one of the chapters was, essentially, that if you don't address the people issues in computer security, you're missing half of the problems. When I repeated that message at a recent meeting with executives and said that I thought that was still true today, I was criticized because, as one executive put it: "You greatly understate the human contribution to the problem — it is far more than 50%!"

Reprint 58232.

MITSloan
Management Review

PDFs ■ Reprints ■ Permission to Copy ■ Back Issues