



July 16, 2001

Special Report: E-Commerce

The Privacy Officer

What's standing between your personal information and the world? People like Benjamin E. Robinson III

By JARED SANDBERG

Benjamin E. Robinson III probably knows more about you than you know about him.

As chief privacy officer of MasterCard International Ltd., he is the keeper of all manner of sensitive financial information about MasterCard carriers. Mr. Robinson is among the growing numbers of chief privacy officers, a newly created executive post popping up throughout corporate America. Companies like **American Express Co.**, **Sony Corp.**, **Citigroup Inc.** and **International Business Machines Corp.** have appointed their own privacy chiefs. Today, there are an estimated 300 of them, and their numbers are expected to swell over the next few years.

Detractors call the appointing of CPOs a public-relations ploy or a case of the fox guarding the henhouse. They agree somebody has to look after consumer privacy. They just aren't convinced it's the companies that should be doing it.

Whoever is the guard, electronic commerce clearly has made the job an important one. E-commerce depends on collecting and sharing an unprecedented amount of sensitive information. For companies to succeed in the e-commerce business, they must flesh out details of their customers' otherwise anonymous digital personas. Collecting information about consumer preferences -- which products people buy and those they're likely to buy -- can allow e-merchants to offer convenience unrivaled in the offline world. By tracking prior purchases and recognizing repeat users, Amazon.com, for example, is able to promote a strikingly tailored range of products to customers revisiting its site.

Need to Know?

But with the increase in companies gathering data on their customers has come a growing concern about where that personal information is going.

Lawsuits against companies charging privacy violations, including some filed by state attorneys general, are on the rise. Most commonly, plaintiffs are taking companies to task for violating their own privacy policies by sharing customer data. Up until last year, such suits were unsuccessful, but the courts have begun to rule in favor of plaintiffs more frequently, reflecting judges' sensitivity toward the public's growing privacy concerns. The newsletter *Privacy and American Business* estimates that companies have paid \$61.5 million in settlements of such suits since 1999.

Meanwhile, the Gramm-Leach-Bliley Act, signed by President Clinton in 1999, requires the financial industry, including credit-card companies, brokerage services and travel agencies, to notify consumers of their privacy policies. They also must allow consumers to "opt out" of practices in which companies disclose certain financial details to other companies. That is, consumers must be able to tell companies to keep private any personal information.

It's the chief privacy officer's job to keep a company out of hot water -- whether in a court of law or in the court of public opinion. Some CPOs may come from the government-affairs department of a company, the legal department, consumer affairs or the information-systems group. But all of them must help their companies avoid consumer litigation, assess any risks to customer privacy and develop Internet privacy policies. They also must create a system that will handle and resolve consumer complaints and make sure new products don't threaten customer privacy.

Simply put, CPOs have to protect consumers from their companies while protecting companies from consumers.

Politics of Privacy

It's trickier than it sounds. CPOs must balance their customers' right to privacy with their corporation's need for profits. And the two don't necessarily go hand in hand.

"How do you mobilize support when you're stepping on the bottom line and you know powerful people are going to be your foes?" says Alan Westin, president of the Center for Social & Legal Research, a Hackensack, N.J., organization that publishes the *Privacy and American Business* newsletter and has conducted training sessions for CPOs. "If you are not good at people skills, at coalition building, at using the political environment to show top management what it must do, then you're in the wrong job."



John Patrick Naughton

The Quiet Man: Benjamin E. Robinson III, MasterCard's CPO

Not Mr. Robinson. As the 37-year-old executive strolls the white-marble headquarters of MasterCard, set amid the stately oaks and maples of Purchase, N.Y., he greets everyone, chatting with each person he meets about personal affairs. Mr. Robinson's congeniality, his light touch and big smile, come in handy for a typically politicized post. He balks at the notion that his job puts him between a rock and a hard place, in large part because conflict isn't his style. He says he never has arguments over the cost of privacy compliance. "Usually, I get, 'Fine, make it happen,'" he says.

As an association of member banks, MasterCard hasn't traditionally dealt directly with consumers. It has known only credit-card numbers -- data that are protected in a hush-hush facility in St. Louis -- and nothing about the people behind them. Only the member banks knew the customers' names. But with a growing number of online products and services, the company is dealing directly with its customers, attaching addresses, phone numbers and even purchases to the card numbers.

There are moments when Mr. Robinson has had to play the bad guy. Take MasterCard's Online Exclusives offering. If users sign up for the service -- supplying their names and addresses, among other details -- they can receive discounts from dozens of e-commerce merchants. You can get a 10% discount, for example, at MoroccanLanterns.com if you use your MasterCard. But for MoroccanLanterns.com to qualify for the service, the Dallas company had to comply with MasterCard's privacy policy, which says the only reason a partner can share data with another company is to fulfill a customer order. So in the case of MoroccanLanterns, the company can give its suppliers the customers' addresses and product specifications only to produce and ship a lantern. It can't share the information with, say, a company selling light bulbs.

In the year that Mr. Robinson has held the post, he has scotched about a half-dozen proposed partnerships because he lacked confidence that the partners could keep a lid on sensitive customer data. Though he concedes he may have locked horns with colleagues who were pushing such partnerships, he doesn't see any evidence of rancor. That may be because he's convinced them of his motto: "Good privacy is good business."

"The CPO position doesn't have to be adversarial," he adds. "It's not my personality or style to take disagreements personally." For Mr. Robinson, the job is largely about finesse. When he missed an important marketing meeting, he sent its organizer flowers.

Perhaps his greatest challenge is making sure that as MasterCard offers more and more consumer services in which a great deal of information about the cardholder is known, the personal details of the holder doesn't spin out of control in the ether of the Internet. An online merchant could pass the data along to a direct marketer, who, in turn, could pass it along to yet another company. This "data flow" concerns Mr. Robinson most. E-commerce has "nuances that we never necessarily thought of," he says. "Cyberspace is so broad that we don't know where the information is going."

Mobile Concerns

On one recent morning, after his requisite cup of coffee, Mr. Robinson sat down with separate MasterCard businesses that make up the so-called E-Business Group. Included among the meeting's participants were people from various emerging technology divisions such as those involving smart cards, which have built-in microprocessors and memory and are considered more secure than credit cards, and mobile commerce, which involves purchasing products through cell phones and other wireless products.

The meeting's big issue: how the Federal Communications Commission might regulate the nascent arena of mobile commerce. Like many of his CPO counterparts, Mr. Robinson spends much of his time schooling colleagues on existing privacy regulations or anticipating potential new rules.

It was Mr. Robinson's task to sift through current regulations and look for a hint. But no such luck. "No one has really talked about" privacy and mobile commerce, he says.

So he points out -- as he had done many times -- that if consumers use new technology that involves MasterCard, the company will have to draft a privacy policy, notify users of the policy and give them a chance to opt out. "A lot of these meetings at this stage of the game are giving the business units an idea of what's going on in the [privacy] industry," he says.

After that hourlong meeting, Mr. Robinson headed into the office of Ruth Ann Marshall, president of MasterCard's North America Region, to talk about hockey. In March and April, MasterCard ran a sweepstakes with the National Hockey League that allowed cardholders to win free passes to the league's Celebrity Face Off game. Since the contest dealt directly with the personal information of Canadian consumers as well as those in the U.S., Mr. Robinson needed to ensure that the company's U.S. privacy policy would meet the requirements of Canadian laws.

It didn't. Like the U.S., Canadian laws require businesses to notify consumers how their information is being used and give them an opportunity to stop it from being passed along. But the Canadians go further. Any consumer in Canada can request access to the personal data being collected by a company. So Mr. Robinson recommended that MasterCard prepare to give Canadian residents access to their digital selves. That meant contacting information-systems staffers to make sure each person's data could be segregated out and shipped if requested -- which staffers did, for Canadian participants only.

Global Differences

Such subtle differences between privacy laws world-wide pose a constant challenge. Last year, for example, MasterCard unveiled the TradeCard, a credit card that prequalifies companies to buy goods and services from international companies without going through the lengthy process of obtaining a letter of credit. Mr. Robinson was concerned that some countries, such as Hong Kong, give privacy protections to businesses. Unlike with consumers, businesses in the U.S. don't necessarily have to be informed of the fact that their private information may be passed along to other businesses. He made sure MasterCard notified its TradeCard users of the possibility of their information being passed along to other TradeCard members. The company also told users that it wouldn't share a member's information outside the TradeCard offering without the member's consent.

After the meeting with Ms. Marshall, Mr. Robinson headed to the cafeteria for a working lunch with MasterCard's audit team. Toting a packed lunch in his signature fluorescent green bag, he sat down with a group responsible for reviewing the company's business practices. It was a simple meeting to report to him their review of different divisions, making sure the proper privacy policies and procedures were put in place in all the divisions that needed them. In the year Mr. Robinson has held the post, he's crafted about 10 different privacy policies, each catering to the laws of the countries involved.

The auditors, who were making sure MasterCard's units had complied with the Gramm-Leach-Bliley Act, said Mr. Robinson has done a good job. So far, it appears Mr. Robinson is doing something right with respect to privacy: The company says it hasn't received any customer complaints.

-- Mr. Sandberg is a staff reporter in The Wall Street Journal's New York bureau.

Write to Jared Sandberg at jared.sandberg@wsj.com¹

URL for this Article:

<http://interactive.wsj.com/archive/retrieve.cgi?id=SB994959146618010786.djm>

Hyperlinks in this Article:

(1) <mailto:jared.sandberg@wsj.com>

Copyright © 2001 Dow Jones & Company, Inc. All Rights Reserved.

Printing, distribution, and use of this material is governed by your Subscription Agreement and copyright laws.

For information about subscribing, go to <http://wsj.com>

Close Window