## Business Intelligence Journal

# Experts' Perspective

By Sid Adelman, Jill Dyché, Richard Hackathorn, Claudia Imhoff, Lisa Loftis

**As the manager of data warehousing, Rick is struggling with how much is enough in enhancing the customer database. Knowing more about customers increases the effectiveness of marketing campaigns and the quality of service to those customers. However, Rick wonders, "When do we, as a company, go too far and invade the privacy of our customers?" TeenStyle Unlimited is a regional retailer in the clothing industry specializing in apparel for teenagers. It is a volatile business subject to the rapidly changing styles of this age group.**

**Executive management has made the theme "Knowing Our Customer" a major corporate strategy. In the last few months, management increased the priority of this strategy after several successes with targeted marketing campaigns. A major factor in these successes was the enhanced customer data from outside information providers, who offer ever-increasing details about teenagers, such as ages, educational level, school activities, marital status, and traffic tickets. Based on magazine subscriptions, data about the ZIP code, street address, and telephone numbers has been used to identify specific customers in 70 percent of these providers' databases.**

**Management wants to extend this personal identification to likely prospects within certain geographic areas. In addition, management wants to ask customers (at the time of sale) more information about their preferences in return for product discounts. Several similar initiatives are in the pipeline.**

**Despite the potential seriousness, management wants to keep the privacy issue quiet, discussed only within a small group of executives. The general consensus is that this information is owned by the company and is not a privacy issue as long as it is used to better serve TeenStyle's customers and prospects. Management has already made it clear that it is not acceptable to ask customers about their privacy preference. Besides, this is the essence of their competitive advantage in a tough marketplace.**

**Rick is not entirely buying the company line. Something seems wrong to him. To make matters worse, the security and oversight of personal information is lax, but he is uncertain about constructive ways to surface and resolve this privacy issue. What factors should Rick consider, and how should he resolve this privacy issue?**

**Claudia Imhoff and Lisa Loftis:**
Rick certainly has a thorny issue to deal with—especially given the underage nature of the most of TeenStyle's customers—but the situation is by no means hopeless. In fact, life parallels nature here in that if he can get past the thorns, he has a thing of value (CRM enthusiasts might also say beauty)—much like a flowering rose bush and the thorns that protect it.

Let's look first at the rose that Rick might find when he navigates those thorns. In this case, the rose is called customer trust. It is a precious commodity many organizations strive for but few actually achieve.

Organizations adopting CRM strategies such as "Knowing Our Customer" are doing so in an effort to stimulate customer loyalty, to increase customer share of wallet, and to maximize customer profitability. Fostering and maintaining the customer's trust is critical to each of these goals. Most customer lifecycle models are developed with trust as a founding component. (The customer lifecycle is a means of defining and communicating the way in which an enterprise interacts with its customers and prospects.) Trust must be built between an organization and a customer to foster the loyalty required to propel the customer repeatedly through the lifecycle and have them acquire additional products and services.

Every interaction that Rick's company has with its customers or prospects is an opportunity to build trust. One way to build this trust is for TeenStyle to accumulate knowledge about its customers, and to earn their trust by using this knowledge to tailor subsequent interactions to better meet customer needs. This postulate holds true whether TeenStyle is interacting with a long-time customer or with a consumer that has yet to move into the customer lifecycle.

TeenStyle's effort to better target and serve customers by enhancing the information it collects with third-party data is clearly a step in the right direction. If applied judiciously, these activities can have a positive impact on the customer experience, contribute to building trust, and provide the customer with a reason to re-enter the lifecycle. More positive yet is the plan to solicit preference information directly from the customer. By beginning a dialog with its customers, TeenStyle is engaging them in the relationship, a great way to build trust. If the store solicits e-mail addresses and clothing preferences from its customers, it can then use the information to earn trust.

Here is an example: sending thank you e-mails that refer the customer to the store's Web site for future sales and contain discounts specifically targeted to their clothing preferences. The dialog has begun with a very positive customer experience. As long as the solicited information is not misused, this interaction can build trust and lay the foundation for long-term, mutually beneficial relationships.

If you are reading closely, you have probably already identified the thorns that Rick must pick through— privacy—and the determination of management to sweep it under the rug. Consider the start of our discussion on trust, which goes like this: "As long as the information is not misused …" This is where the privacy issue becomes critical. According to *Webster's Unabridged Third New International Dictionary*, privacy entails "freedom from unauthorized oversight or observation." The key word is "unauthorized." Privacy does not necessarily exclude oversight or observation, but it does require that such actions be properly authorized.

Organizations build loyalty when their customers trust them enough to give information that will enable the organization to provide personalized service. To engender the trust needed to obtain information that enables the personalized service, companies like TeenStyle must provide an environment in which their customers are comfortable with the way information about them is obtained, maintained, disseminated, used, and secured. What's more, because many of TeenStyle's customers are minors, creating this comfort level and starting dialog must also be geared toward parents as well as the young people who make the purchases.

A privacy policy is robust (and makes customers feel secure) when it contains the following constructs:

- It is visible and clear. The purchaser and/or the customer's parents must be aware of the promises the store is making about preserving privacy, and they must understand the language of the policy. By not wanting privacy to come up with its customers, TeenStyle's management is violating the most important aspect of trust and privacy.
- It describes what information is collected and how it will be used. As long as the

uses are beneficial to the customer, they are more likely to accept its collection and use.

- It identifies any third parties that may receive the information. Just because TeenStyle has gained a customer's trust does not mean that the customer trusts all of TeenStyle's partners. The policy should clearly spell out TeenStyle's intentions here and should provide the customer (and parents) with choices concerning the dissemination of information.
- It provides the customer with update rights. Customers must have the ability to change incorrect information about themselves. This can work in TeenStyle's favor because when done properly, it demonstrates that the company learns from its customer interactions and that enhances trust both for the young customers who are purchasing clothing and for their parents.

If he plays his cards right, Rick can use the rose—the very real and very beneficial opportunity the company has to build customer trust and accrue all the attendant benefits—to help the executives understand the full import of navigating the thorns of privacy. He can attempt to allay some of management's negative reactions to privacy by highlighting that it doesn't have to be viewed as an impediment to CRM. Instead, it should be viewed as a critical and mandatory component of the strategy. He can take the mystery out of privacy by detailing for management the aspects of a robust privacy policy. He can alleviate departmental concerns by emphasizing that the policy should be developed by a cross section of the executive team and should represent a synthesis of needs across all groups in TeenStyle: legal, IT, marketing, and customer service at a minimum. Finally, he can link the positive impacts of a privacy policy to the trust it can establish between company and customer.

He may want to consider pitching privacy like this: "Trust embodies the customer's confidence in TeenStyle's integrity. A customer who trusts our company is much more likely to provide us with information and continue doing business with us, than a customer who distrusts our company. Adopting a privacy policy that reassures our customers that we value their privacy and are dedicated to maintaining it can go a long way toward building trust and enabling us to know our customers and achieve our ultimate goals."

**Jill Dyché:**
The free movement of personal information within and among organizations has certainly upped the jitter factor of an already-wary public. No wonder TeenStyle's management is reluctant to publicize their intent to use personal data for marketing purposes. All the detailed personal data in the world won't amount to much if TeenStyle's customers stop trusting the company and decide to buy their halter tops and cargo pants elsewhere.

Pity the poor data warehouse manager faced with balancing the business value of personal data with the risk of increased customer attrition. Rick has his work cut out for him.

His first task is risk management. Rick should draft a memo to his boss, subject line: Risks of Acquiring and Storing Personal Data. Yes, the memo might initially be misconstrued as the well-worn managerial "CYA" maneuver, but its real purpose is ensuring that executives are educated about the issues involved in the acquisition and tracking of customers' personal information. The memo should crisply outline the pros and cons (including potential legal and PR fallout) of capturing personal data as part of a customer's profile.

Rick should then inventory the various enterprise applications that call for customers' personal data. Target marketing applications, call center dashboards, and inventory management may all request specific consumer demographic and behavior information that transcends the standard name-and-address fields. Understanding why those applications need the data and how it's used is an important first step in justifying its collection.

Such an inventory may also reveal that, in fact, only a single application —a campaign management system, perhaps—requires personal data. Truth is, retailers aiming for the teen market face the reality of a very young, cash-paying demographic where personal information isn't as relevant as aggregated purchase behaviors and where household-level information—moms and dads are certainly making purchases on behalf of their progeny—is more important than individual detail. Rick should know whether the use of personal data is a strategic need or an operational one, enterprisewide or simply departmental, thus requiring a functional data mart and more attention from the company's marketing department or ad agency.

In the case where multiple applications need personal information, the data warehouse operational environment becomes paramount. Rick's team should ensure that the data warehouse infrastructure includes a deliberate design and rigorous business rules that can dictate and limit accessibility of specific customer data based on the application requesting the information.

On an issue with as much impact as consumer privacy, Rick can't act in a vacuum. He should collaborate with his IT management peers to ensure that security measures such as firewalls and password protection are in place. He should have his database design team perform a walk-through of the current design, with DBAs weighing in on access rights.

Furthermore, Rick should encourage his colleagues in marketing to come up with a policy of communicating with customers and giving them a choice. It's important to note here that most of the privacy lawsuits filed against U.S. companies—surely the source of management's unease— have little to do with collecting personal data. Rather, consumer privacy litigation has targeted companies' failure to inform their customers about privacy practices.

TeenStyle shoppers should be clear about the quid pro quo: What do they get for opting in and providing their personal information? What do they miss for opting out? After all, we're not talking about divulging medical records here. The fact is everyone loves a freebie and TeenStyle shoppers won't think twice about sharing a list of their favorite magazines or sitcoms for psychographic research if it means a lip gloss being thrown into their shopping bags.

Since Rick has already articulated the risk-reward scenario, he should consider taking the lead and enlisting a cross-functional team of business managers to draft a formal corporate privacy policy and present it to TeenStyle's executive staff, and board. While this is arguably the tail wagging the dog—the business side should have drafted a formal privacy policy and communicate it to IT— Rick's vision may be the necessary impetus to get the ball rolling. Judging from management's waffling on the privacy issue, it's probably high time.

This gets to the heart of the most worrisome issue: that TeenStyle's executives are reluctant to reverse the policy edict making it "unacceptable" to request customer information to now collecting personal information to bolster marketing initiatives. Management should reconsider its intent to "keep the privacy issue quiet." With proposed legislation like the Consumer Privacy Protection Act of 2002 (H.R. 4678) and the Online Personal Privacy Act (S-2201), both of which require businesses to inform consumers about what personal data is collected and how it's being used, it's only a matter of time before TeenStyle will have to come clean with its marketing practices. The extent to which Rick and his team can enable customer-focused business practices centered around clean, sustainable personal data and a consensus-driven privacy policy is the extent to which TeenStyle can retain happy customers while holding its corporate head high.

**Sid Adelman:**
Let's get inside Rick's head. What are his concerns? What makes him think something is wrong? Why does he feel there is a privacy issue? Is there something unethical going on? Is he afraid of being featured on *60 Minutes*?

Rick is concerned that management wants to keep the privacy issue secret. That in itself is a red flag because we all know that a secret is best kept if only two people are involved and one of them is dead. Rick knows that eventually what is going on will

become public knowledge and Rick will be called to task for helping to keep it under wraps.

Rick also has an uncomfortable feeling about just why management wants to keep it quiet. If there is nothing wrong, why keep it secret? The position of management's not wanting to ask customers about their privacy preferences also concerns Rick. If TeenStyle is trying to know its customers, why shouldn't privacy be one of the characteristics? We already know the answer: it costs money to gather data, and TeenStyle loses some marketing capability for those who opt out.

"Knowing Our Customer" is fine unless we go too far and invade that customer's privacy. So how far is too far? If it helps TeenStyle sell their product, is that a sufficient criteria or is there something else? The outside providers can give us information to help target our teen customers, so let's look at what they can give us to match with our customers and potential customers.

1. Age – may be OK.
2. Education level – does anyone mind? Possibly.
3. School activities – where we can sell outfits to the sports minded? This makes sense.
4. Marital status – hmm?
5. ZIP code – no problem here; this helps us target those with more available credit on their VISA card.
6. Street address – if we are sending mailings, we need it and we will use it for matching customers as long as it's not being used for some nefarious purpose.
7. Telephone number – since telemarketing has been all but outlawed, why do we need it except to match customers?
8. Traffic tickets – TeenStyle must be planning to market its new line of clothing, Outlaw Gals. This is way over the line.

Also, management wants to ask customers about their preferences. This initiative should not be a privacy issue because customers can decline to provide the information.

Rick has another concern, that being security and oversight of personal information at the company has been lax. Apparently, there have been no corporate policies to protect customer information. Let's look back at the data that could be available to some one in either IT or in some other part of the organization. They could do a search on high school drop outs, who are divorced, size 0 (I know what clothes you bought), who live in their geographic area, have had three or more speeding tickets, and at least one DUI in the last two years, and who have preference for leather. They would be able to get a listing with address (I know where you live) and phone number and now the stalker has everything he or she needs. Rick has a real problem and so does TeenStyle.

Rick should be able to terrify, then convince, management about the need for privacy. He needs to make the case to management about their extreme exposure (let's remember JetBlue and their sharing of customer information). Rick's pitch could include a mockup of a newspaper report.

"Knowing Our Customer" is fine unless we go too far and invade that customer's privacy. Rick has legitimate concerns for himself and for TeenStyle, but he should be able to satisfy TeenStyle's marketing requirements and still not violate his own professional and ethical standards. Rick's presentation must contain concrete steps to follow. He should propose the following to management:

1. Establish a strong security policy for customer data that is written and included in training and has teeth ("You will be fired for the following infractions").
2. Customer data should be only available on a need-toknow basis.

3. Unauthorized access attempts would be closely monitored and follow-ups would be made.
4. Build security capabilities into the system and assign authority and responsibility for security of customer information.
5. Limit the data from the outside information providers and the preference data to only such data that will help sales and provide better customer service and avoid data that could be construed as inherently private.

**Richard Hackathorn:**
Rick is concerned, and he should be. TeenStyle Unlimited is probably in violation of the Children's Online Privacy Protection Act (COPPA). As IT professionals, we tend to have limited knowledge about legal and ethical matters, especially in the area of privacy. We tend to analyze the situation from the perspectives of technology or marketing, not realizing the much large societal context. A compliant or even a simple enquiry from one of their customers (who happens to be 12 years old) could launch a court proceeding that could appear vividly on the front page of the *Wall Street Journal*.

In 1998, COPPA was signed into law and applies to commercial Web sites collecting information from or about children under 13. These sites are required to provide privacy notice about the collection, use, and disclosure of children's personal information. Most sites also must obtain "verifiable parental consent" before using this information. COPPA became effective in 2000, carrying civil penalties of up to $11,000 per violation. 1

What does this mean for TeenStyle Unlimited? Let's look at three commercial Web sites that deal with the COPPA situation. First, consider a site that avoids any information about children. Toys "R" Us will not collect any such information, as noted in its Privacy Statement: *The Online Stores and the "R" Us Sites do not knowingly solicit or collect personally identifiable information online from children under the age of 13 without prior verifiable parental consent. If any "R" Us Family Member learns that a child under the age of 13 has submitted personally identifiable information online, in contravention of these measures, it will take all reasonable measures to delete such information from its databases and to not use such information for any purpose (except where necessary to protect the safety of the child or others or as required by law).2*

Likewise, Amazon.com will not handle any requests from persons under 18: *Amazon.com does not sell products for purchase by children. we sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian.3*

Second, consider a site that collects information but only temporally. Colgate-Palmolive Canada Inc. offers a "Tooth Fairy" service for young kids, but the data stays about as long as the tooth: *Only a few features collect your child's E-mail address, and then only for the purpose of responding to your child's request or answering your child's question. Once we have responded, we delete your child's E-mail address from our system. 4*

Third, consider a site that does collect information from children, their primary clientele. Claire's recognizes their obligations but cuts a few corners: *At Claire's Stores, Inc. we are committed to protecting the privacy of our users, especially that of children ages 12 and under. This privacy policy details the type of personal information that is collected from visitors to our site, how it is used, and special considerations which are made to ensure the safety of children on [our web site].5*

In the situation of a Wish List, the child is asked to give a "Made Up" name: *We also allow our users to save their wish lists for access at a later time. To save your wish list, you will be prompted to supply an anonymous username and password.*

However, for any purchase, a big assumption is made. The person is assumed to be an adult to use a credit card. Finally, we allow users with valid credit cards to purchase gift cards for their friends and family. Finally, Claire leaves the door open to a possible loyalty program in the future.

In the future, Claire's may create a loyalty and club membership program, where users will be asked to provide their first and last names, birth dates, a postal address, an e-mail address, and a telephone number.

The lesson is that privacy is a major issue throughout most of the world. Companies must be smart about their practices for handling personal information, which are dependent on many factors, such as age. Informed ethical standards and legal compliance lead to good business practices. Ignorance is not an excuse!

1. *A PDF version of COPPA is at http://www.ftc.gov/os/1999/10/64fr59888.pdf along with a concise How To Comply With COPPA from the Federal Trade Commission at http://www.ftc.gov/bcp/conline/pubs/buspubs/ coppa.htm. Good layperson description can be found at ParentsDirect.net (http://kidsdirect.net/PD/privacy-act/).*
2. *http://www1.toysrus.com/guest /rusFamiPrivPolicy.cfm*
3. *http:www.amazon.com/exec/obidos/tg /browse/-/468496/103-8351141-7898250*
4. *http://www.colgate.ca/english/legal /index.html*
5. *http://www.claires.com/privacy_ printfriendly.html*

Top printable format