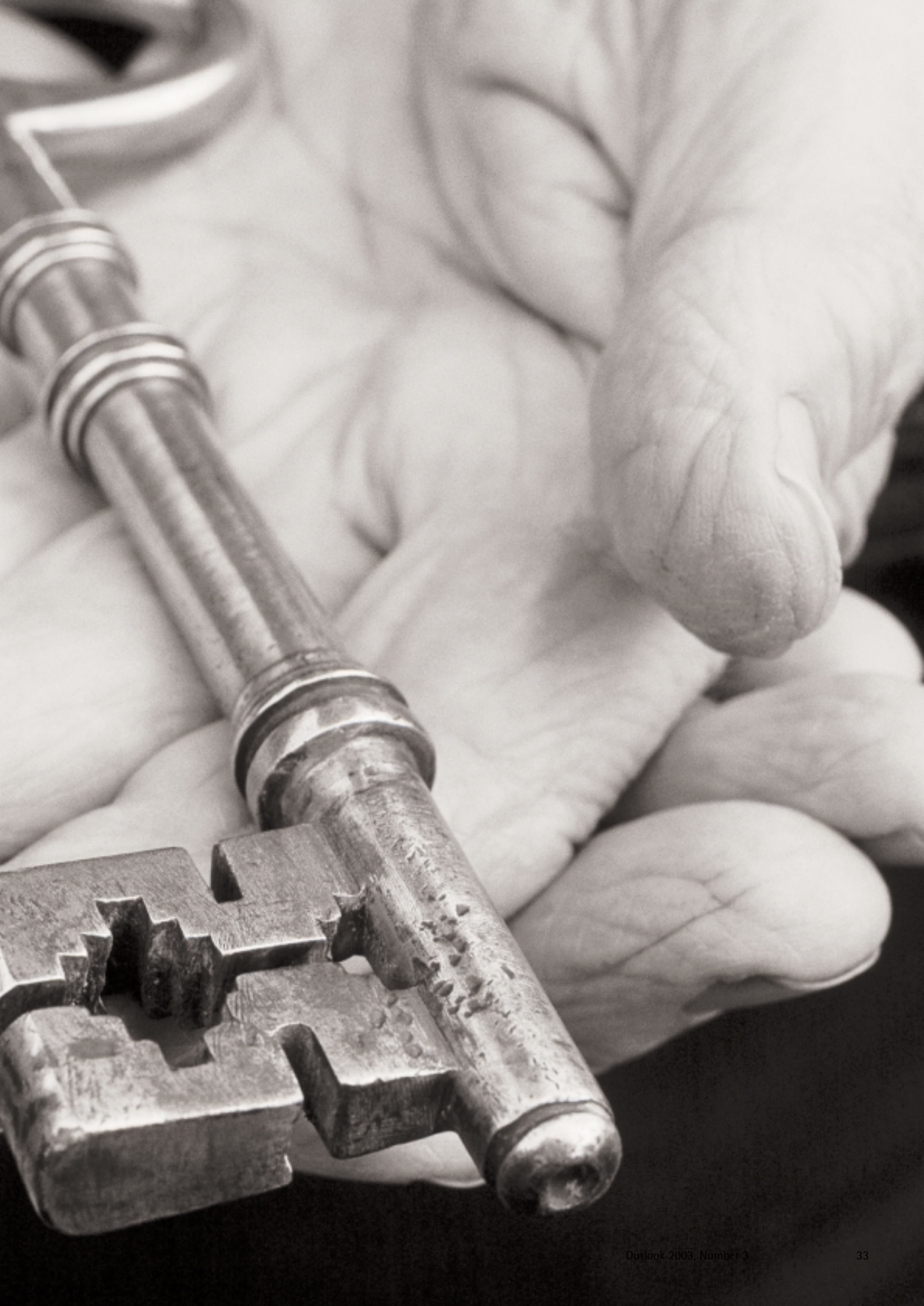
Technology

The economic value of trust

By Andrew E. Fano, Sanjay Mathur and Baiju Shah

Today's technologies provide companies with unprecedented access to customer information—and raise serious concerns about privacy. By taking a deliberate approach to building customer trust, a business can turn the privacy challenge into a significant competitive advantage.



Can personal privacy survive in an age when business and government alike have more technologies at their disposal to know more and more about us?

Today, there is mounting tension between two defining aspects of 21st century commercial life. On the one hand, consumer data and information play a vital role in the successful operation of almost every business. On the other hand, most of us are heirs to a long-standing belief in an individual's right to privacy as well as to the idea that people should have a measure of control over the information they generate as consumers.

At some point in our lives, most of us have experienced the technology-privacy trade-off—and the lingering anxiety that comes with it. As consumers, we like the convenience of online financial transactions and would like to be able to trust that the information we provide will be used responsibly—but we can't always be sure this will be the case. We like the idea of in-vehicle telematics services that dispatch emergency help automatically when needed—but, of course, we don't want similar technologies used by law enforcement and insurance companies to monitor our driving habits. We are intrigued by services that keep track of our preferences and buying habits to offer us special deals or even shop for us—but we wonder who else is tracking our purchases at the supermarket, the pharmacy, the movie theater.

These represent legitimate and pressing concerns for consumers, and complex issues for business and government. How can companies overcome such concerns to offer new services, improve customer relationships and capture new markets? Accenture believes a vital component has been missing from the privacy debate: a proactive business perspective focused not merely on compliance with laws that protect privacy but also on the notion that companies can earn consumer trust. In return for access to information, the company that has earned trust can assure consumers and business partners that they will use that information responsibly to provide value-added services. Implicit in this response to privacy concerns is the belief that trust has an economic value to companies and that it can be used to win competitive advantage.

If companies are to use today's revolutionary technologies effectively to fuel economic growth, they must meet the privacy challenge head-on. Today, privacy and trust have become critical aspects of any business imperative, including brand management, customer relationships, profitability, research and development, capturing new markets and even economic expansion itself.

Keeping track

One thing all parties in this debate can agree on: In most parts of the world, technological change has overwhelmed the ability of most current laws and regulations to protect privacy.

Today, the amount of information gathered about individuals is growing through the proliferation of surveillance cameras and sensors; microchips and radio frequency identification (RFID) tags embedded in devices and products; wireless devices that provide location data; and smart cards and interactive TV that can track viewing and buying preferences. In addition, advances in electronic storage mean that companies and government agencies can hold on to more information

about people. Meanwhile, the Internet provides the ultimate copying device, making this information easily available to millions. Because the commercial value of personal data has been recognized, companies now have considerable financial incentives to take the time to gather information and to use machine-learning technologies and data-mining techniques that can make inferences about customers based on their private information.

The benefits of these technologies are becoming clearer every day—benefits that are not just consumer-oriented but have enterprise dimensions as well. For example, The Gillette Company has been at the forefront of implementing RFID technology, and it plans to embed hundreds of millions of these miniature tags in its shipping cases. Why? Because this technology promises to revolutionize supply chain management, specifically to improve loss prevention.

Take this development a step further and put RFID tags on the products themselves, and you can track them from the factory to the warehouse to the retail store. You can control inventory more easily and also reduce shrinkage and misdirected shipments. In fact, Accenture research has shown that the use of an RFID-based system across a retail supply chain can yield 99 percent inventory accuracy and eliminate 95 percent of the labor involved in the cycle count.

Yet resistance from privacy groups to tagging technologies at the consumer level only begins to suggest the challenges ahead. In April 2003, clothing retailer Benetton Group announced that it was postponing plans to embed RFID tags in one of its clothing lines. This decision signaled to many companies that they need to do more about privacy than just understand relevant legislation. They need consumers to trust them to protect their personal information.

No one should look at these developments naively. Technologies are more intrusive today, and they will only get more so. The personal information gathered to gain insight into consumer preferences can be put to positive use serving people and the business community; it can also be used in damaging ways. That information you provide to make an online purchase, for example, can be used by a criminal to steal your electronic identity. The same e-mail function that is so valuable to millions can be abused by unscrupulous businesses to the point that the channel is rendered useless.

Critical balance

It all comes down to this: How do companies balance risk and benefit? And which of the various stakeholders in a commercial relationship should take which responsibilities to help maintain that balance?

Individuals could retain the entire responsibility themselves, but that's

Government is only part of the answer. At best, laws and regulations will inform companies about what practices are and are not legal.

Building trust into your business and technology solutions

How can basic guidelines about trust (see story) be designed into a business and technology solution? Several prototype solutions designed at the Accenture Technology Labs demonstrate these principles at work.

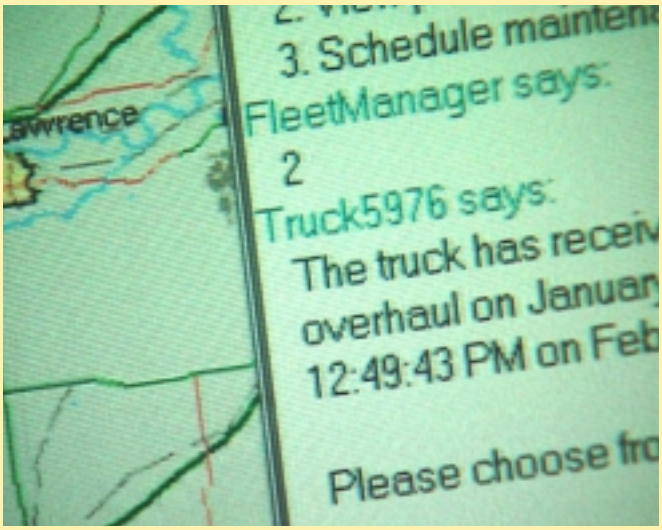
For example, the Accenture Object Information Exchange prototype demonstrates how enterprises can use a permissions-based approach to share data about an asset across locations and with external business partners. Take applications related to fleet management, for example (below, left). An "intelligent" truck, equipped with sensors, communicates information about its status, such as location, availability, maintenance requirements and cargo details. Yet access to the complete range of information is restricted; partners in the supply chain get only the information they need to perform their tasks efficiently.

This responsible and trustworthy use of information maintains accountability and offers a degree of protection against fraud and other misuses of information. Accenture Technology Labs has worked with a number of clients to pilot similar fleet management solutions based on these principles.

Or consider a consumer application such as the Accenture Reality Instant Messaging prototype (below, right), which integrates instant messaging with television programming in real time. As a viewer watches a music video, for example, the TV network might offer a free subscription to a music video instant message session. In deciding whether or not to join the session, the viewer weighs various incentives: targeted offers for CDs and related merchandise, information about the artists and the ability to chat with friends who are watching the same program.

This solution demonstrates the principle of offering relevant value to consumers in return for the trusted use of a portion of their personal information. Customers decide upfront what level of information about their identities and preferences they are willing to share with the network in exchange for services they value. Retailers benefit by gathering real-time insights into customers' interests and reactions, as well as by extending promotional offers through a relatively new and popular electronic channel.

A critical aspect of trust building in this solution is the groundwork that must be laid by an organization to provide assurances that all business partners in the value chain abide by the same high principles. If a person using this solution is suddenly deluged with unwanted phone calls and e-mail from related companies, you can bet that's a customer lost forever.



more of a burden than it might seem. Do consumers want to be asked every time a company wants to use a certain bit of their data, or would they rather find a company they can trust and give it permission to use their information under certain specific conditions?

Consider one widely used technique for giving consumers control: the opt-in/opt-out method. Rarely is it a happy choice. In practice, opting in to a service means giving up control not just to one company but to a battery of that company's business partners that may *not* have agreed to be responsible with the individual's information. Users of a popular online lending company have found that their spam e-mail rose dramatically in the weeks following their initial dealings with the company—not a good way for this business to establish itself as a trustworthy user of information. In effect, the choice is between getting no service at all and throwing your information to the far winds.

Another way to control risk is to keep rewriting legislation as technologies evolve. Privacy laws are an important part of the mix, to be sure. In some countries, for example, consumers have the legal right to access and correct misinformation about them, and to be told the reasons for credit decisions. Other laws set limits on how long personal information can be stored. Some legislation can enhance competitiveness; for example, laws that restrict the misuse of customer channels may have the effect of making legitimate channels to the customer more effective and valuable.

Yet an answer that relies solely on the government will often have unintended consequences. In the United States, for example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is part of a larger legislative effort to make it easier for individuals and small businesses to get and keep health insurance. With nary a touch of irony, part of the act, which took effect in April 2003, includes an "administrative simplification" section to encourage electronic transactions that, in turn, have generated a host of new regulations to assure the security and privacy of electronically stored medical data.

Entire careers are being made today helping companies figure out how to comply with this act. HIPAA has had a profound effect on hundreds of compliance issues, including workers' compensation and medical savings accounts. Even at a personal level, the effects can be jarring. For example, the law significantly restricts the ability of adult children who are caretakers of elderly parents to talk to their parents' doctors.

Even when the compliance issues are straightened out, legislation can be beset by loopholes and misuse, or it may be toothless because it carries with it no means of effective enforcement. Moreover, given the pace of technological change, as well as the complexity of each new advancement, efforts to protect privacy through legislation can hardly be expected to keep up.

Not surprisingly, government regulation also tends to be a one-size-fits-all proposition. By preventing the sharing of personal information or the initiation of contact with potential customers, privacy laws can protect consumers who do not want their personal information to be shared at all. At the same time, however, these laws prevent willing consumers from sharing a degree of access to their data to benefit from the kinds of con-

The company that can establish a reputation for providing valuable services while using personal data in trustworthy ways has a significant advantage over competitors.

Today's technologies and services make it harder to hide untrustworthiness and a bad reputation.

text-rich services that modern technologies can provide.

The dimensions of trust

In the end, government is only part of the answer. At best, laws and regulations will inform companies about what practices are and are not legal. What's needed is an approach that doesn't force companies to forgo the use of personal information and access, but rather encourages them to deploy new levels of service in a manner that engenders trust and comfort on the part of their customers. It's in that sense that we speak of the economic value of trust.

Think of it this way: What would you need before you granted a commercial entity significant access to your personal data—your preferences, your transaction history and perhaps your current location (via a global positioning system capability on your mobile phone)? Answer: You would need to trust that entity.

What is trust? In the context of information technology and the business use of consumer data, trust is the confidence consumers or organizations have that a company will respect their privacy concerns and handle their information responsibly. The dimensions of this trust include:

- **Security.** My personal information is being protected against theft or unauthorized use.

- **Data control.** I have control over who gains legal access to my personal information as well as when they get access and what they can do with it.

- **Personal access.** I have control over who contacts me, and how.

- **Accountability.** When I grant access to my information, I know that this access will be used responsibly and in my best interests. If it is not, someone will take the responsibility for the misuse or for the presence of incorrect information about me and promptly take corrective action.

- **Benefit.** The company is not just using my data for its business advantage but is offering me reciprocal benefits that are directly relevant (that is, the information is clearly necessary to the service being provided).

The company that can establish a reputation for providing valuable services while using personal data in these trustworthy ways has a significant advantage over competitors. Its brand is more valuable; it has more opportunities to attract and retain lifetime customers; and it can become a preferred partner in a larger value chain of goods and services.

Can your company become a trust leader—a company with a reputation for responsibly and effectively managing the personal information of consumers and business partners, much as a bank manages the financial assets of its customers? The payoff for trust leaders could be substantial. These companies would be able to negotiate with individuals for the right to aggregate personal information and make it available to other companies. A key aspect of this approach is that all services would be permissions-based, so individuals would be able to leverage their information. In return for the rights to differing levels of information, companies could offer consumers certain discounts or additional services.

Or can your company become the trust leader in providing those permissions-based services within your industry? Becoming such a company means being innovative and savvy

with regard to today's technologies and their potential business and consumer capabilities. Yet the real challenge is in making a plan to establish and maintain your trustworthiness, convincing customers that you have their best interests in mind.

How is trust earned and maintained? Here are some general principles to bear in mind.

Trust is earned over time. A company's history helps consumers determine whether they can trust the company with their personal data. It is for this reason that established companies have an edge over newcomers. A successful incumbent builds on its familiarity; its starting line in establishing trust may put it way ahead of a company that's new to the marketplace (to say nothing of a company whose reputation is less than sterling). At the same time, however, new companies providing new services can make faster inroads into the marketplace by quickly establishing themselves as trustworthy.

Trust can be monitored by governments but not established by them. This is a critical point about the relationship between the public and private sectors. As we have noted, privacy laws (and the investment in enforcement that should, but too rarely does, support those laws) are an important part of the solution. But companies themselves must take the lead in establishing their own trustworthiness.

Trust is an aggregation of many people's experiences. Today's technologies and services make it harder to hide untrustworthiness and a bad reputation. Online auction house eBay offers a particularly good example of this dynamic. Here both buyers and sellers accumulate ratings as to their trustworthiness, which, in turn, affects their ability to transact business effectively on the site.

Trust can take years to establish but can be lost in an instant. Efforts to establish trust can be undone quickly. Consider the true story of one hospital that installed a wireless badging and locating system that was supposed to help find the right people at the right time to assist in emergencies. In fact, the surveillance capabilities of the new system were too much for hospital administrators to resist; it was used to fire a staff member. The result: a rather devastating loss of trust. The nurses' union forced the hospital to unplug the system, so patients now may never experience the benefits it could have delivered had it been implemented in a trustworthy manner.

Trust extends throughout the value chain. Delivering a context-rich service most likely involves a number of business partners, which means that a consumer transacting with a company is transacting with everyone that company does business with. So a company that gathers information about its customers needs to take responsibility for the full use of that information across the business delivery system or value chain.

Part of building trust therefore involves making business arrangements only with organizations whose policies and protection technologies are consistent with the company's own. It will also mostly likely involve establishing a set of self-regulated censures and penalties within industries for companies that breach consumer trust. Binding agreements about the use of consumer information may be necessary through such means as service level agreements.

What practical steps should companies take today to move toward an

Trust may become an important part of a balanced scorecard of intangibles such as brand perception.

It is in the best interests of companies to regulate themselves through the systematic development of trust.

operating model based on trust? Here are a few.

1. Plan your trusted services. Trust doesn't simply happen. As part of your business plan, decide what sorts of trusted services you wish to plan, develop and deploy. Consult with technologists and business visionaries in your industry. Understand the particular technologies and bundled sets of services that will be your new business reality. When technology enables you to reach your customers anytime and everywhere, what will you be able to sell them that's different than what you sell them today? Understand trust on the basis of those future capabilities, not just on your capabilities today.

2. Understand trust in *your* customer base. Clarify the unique concerns and motivations of your customer base when it comes to trust. Different types of business models may have different levels of concern when it comes to privacy and trust.

If you are in a "high trust" business—the medical and pharmaceuticals industries, for example, or financial services—your approach will differ from the approaches used by other kinds of companies. New customer insight capabilities developed in recent years as part of advanced customer relationship management are certainly valuable, as are marketing techniques that help companies better understand their customer base. A 360-degree approach is also vital: Listening to your customers is important, but letting them know the specific ways in which their comments have made a difference is just as important in establishing high levels of trust.

3. Make your trust policy and approach clear. Develop and publish a set of guidelines about how you plan to protect your customers' personal information and privacy. Then conduct an internal audit of these guidelines and enforce them both internally and with your business partners.

One parallel in the United States is the Graham-Leach-Bliley Act of 1999, which informs consumers about the privacy policies and practices of financial institutions, so they can use that information to make choices about the companies with which they wish to do business. A reputation for trustworthiness is likely to be a similar basis of consumer choice. Trust may also become an important part of a balanced scorecard of intangibles such as brand perception. Customers and investors will reward companies based upon the audit of these intangibles.

4. Become part of a trusted value chain. Work with your business partners so that all of you are collaborating to provide the same degree of trust and responsibility across the value chain. It may be possible to construct a hierarchy of trust: Once a customer establishes a trustworthy relationship with the top tier, he or she is assured that all subsequent tiers can also be trusted.

How does one ensure the continued optimization of such a trust chain? An interesting parallel here is UCCnet, a service that allows a company to improve supply chain efficiency by ensuring that all of its trading partners have access to accurate, up-to-date and industry-compliant trading information. Such a concept could be expanded to include policies related to privacy and trust.

5. Be trustworthy *within* your organization as well. Your workforce will model the behaviors established by leadership. To estab-

lish trustworthiness externally, you will need to establish it internally as well.

6. Engage relevant governing agencies. Actively monitor legislative and regulatory developments and demonstrate to the appropriate governing bodies and privacy advocates that as you design and implement new services you are also taking active steps to promote trustworthy and responsible use of consumer data. An effective relationship between the private and public sectors today entails more than businesses simply working with government agencies to establish appropriate privacy protections. It also means working to ensure that governments do not needlessly restrict people's access to the kinds of capabilities available to them through technology.

7. Start now. As we've noted, it takes time to establish trust. Make a plan and get started.

Because the proliferation of technologies and the fear of abuses like identity theft have heightened legitimate concerns about the privacy of individuals and their data, many companies today are reluctant to use information to serve their customers and to make new kinds of markets. Dangers and risks do exist, but there are also dangers in being too timid and risk averse.

Under these circumstances, it is in the best interest of companies to regulate themselves through the systematic development of trust. A consumer-centric and trust-based approach to the technology and business future offers the greatest potential for individuals, companies and governments to take advantage of the revolutionary technologies that are available to them. At the same time, this approach can mitigate the fears of those who know that power over data corrupts, and that absolute power over data corrupts absolutely.

By working in concert with privacy advocates and governments, it is possible for business to have a significant voice in shaping the future of technology and commerce in such a way that consumers are both well served and protected against unwarranted intrusiveness. Privacy can become less of a hurdle to overcome and more of an opportunity for businesses to differentiate themselves, increase their financial value and even energize entire economies. ■

About the authors

Andrew E. Fano is a Chicago-based senior researcher and associate partner at Accenture Technology Labs. Dr. Fano, who has a doctorate in artificial intelligence from Northwestern University, has led a variety of ubiquitous commerce (u-commerce) and information insight research projects. His current research focuses on near real-time insight applications that exploit the context of a person, location or enterprise.

andrew.e.fano@accenture.com

Sanjay Mathur, a senior manager at Accenture Technology Labs, is the global lead for the Labs' information insight research and development initiative. His current projects involve applied business analytics, such as knowledge integration and discovery, dynamic pricing, privacy and trust, and identity and rights management. Mr. Mathur is based in Chicago.

sanjay.mathur@accenture.com

Baiju Shah is a Chicago-based manager at Accenture Technology Labs, where he leads the Labs' market acceleration program. He also conducts research in the areas of privacy, trust, web services and smart object services. His research and technology perspectives have been featured in several journals, including *MIT Technology Review* and *Industry Standard*.

baiju.shah@accenture.com