

Personal data access: Not easily done

Jay Cline

June 3, 2002 ([Computerworld](#))

One of the cornerstones of data privacy is that companies grant people access to the information they keep about them. As reasonable as that sounds, it will be the last privacy cornerstone actually hefted into place. Why? Because providing a single view of each employee and customer is a huge financial and cultural proposition for Global 100 corporations, guardians of the world's most extensive stores of personal information.

The ideal of data access is trumpeted in almost every privacy law. Europe says companies must tell inquiring people what categories of information they've collected about them, where they got it from, what they're doing with it, and who it's been sent to. Canada says ditto, while Australia is satisfied with providing access to the records that have been collected. In the U.S., the Children's Online Privacy Protection Act says parents must have read/write access to data collected online from their preteens. The bars have been set.

But are they feasible? If the Global 100 suddenly attempted to meet the letter of these laws, it would create an IT crisis of Y2k-like proportions -- but with less hope of success.

One reason for pessimism is the stubborn pervasiveness of paper forms. In part for legal reasons, large companies keep paper records on an employee across payroll, benefits and training departments, in addition to supervisors' performance reviews. Collecting all the paper-based, personal information on a single employee would be the private sector's equivalent of meeting a Freedom of Information Act (FOIA) request. Any government worker will tell you that FOIA requests consume numerous man-hours.

The technical barriers facing comprehensive access to personal data are similarly daunting. Even if a company's data flows are mapped, any particular data field -- such as "name" -- may exist in multiple formats reflecting divergent business requirements. Data will reside in systems

based on incompatible technologies that are linked, if at all, at great expense. Providing one view of the individual makes Y2k look like a light warm-up.

Organizational culture is an even larger obstacle to integrated data access. Employees who are closest to a company's customers will feel a natural obligation to guard their data from the company's other regions and lines of business. They can do so by storing data locally and not participating in companywide data systems. Comprehensive access won't occur without their cooperation. These employees have the right instinct -- a bias for privacy -- that highlights a largely overlooked contradiction: Access requirements pit privacy against itself, by encouraging integration of personal data rather than compartmentalization.

Personal data access also requires a heavy investment in information security. Front-line business units won't give up control of their customers' data unless they are fully confident in the security and privacy of the data warehouse. They will need regular convincing that the data store is protected like Fort Knox and that the use of their customers' data for marketing is strictly controlled. Whether most large organizations can meet these internal expectations is an open question.

Running up against these high hurdles, corporations will have to choose: duck or jump. Ducking is very attractive and may be the only feasible, short-term option. Most major companies are doing so. Just one-third of the Global 100 addresses the access principle in their privacy policies posted online. Of those that do promise access, 21 say this applies only to information collected from their Web sites. Only 18 of these companies provide online access to view and update at least part of the information they've collected about customers. None of the Global 100, however, promises online access to all the data they have on you. Privacy heaven has no inhabitants.

Those who duck will stay out of trouble, but those who leap will bury their competition. Creating a real-time, comprehensive profile of every customer enables highly targeted marketing campaigns. Pitching the right product to

the right person at the right time results in lower campaign costs and higher average sales. Highly segmented marketing makes it possible to offer steeper discounts on a regular basis, heightening the barriers to the customer to leave for another brand.

Similarly, knowing more about employees enables more tailoring of benefits packages and thus improving employee satisfaction. Consolidating access channels to customer and employee profiles makes account self-service possible and results in leaner contact centers and help desks. Add this all up, and you create a pricing advantage and a huge technical barrier for rivals to enter your market.

Privacy headlines will continue to focus on rogue data collection and frightening security breaches. But the big story on data privacy is who is going to lead the way on comprehensive data access.

Cline manages data privacy at [Carlson Companies Inc.](#), a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. Contact him at privacy@computerworld.com.