

BY SARAH B. HOOD

**WHAT AMERICA DID** Shortly after Sept. 11, 2001, the U.S. federal government enacted the U.S.A. Patriot Act as an anti-terrorism measure. The legislation erases many boundaries between ordinary police investigations and those of national security agencies, and facilitates the process of obtaining records that could relate to international terrorism. For business, a salient point is that the act makes it much easier for the Federal Bureau of Investigation to demand personal information about customers from such organizations as financial institutions, telephone companies and Internet service providers.

**HOW IT AFFECTS YOU** Under the Patriot Act, U.S. agencies could examine personal data that your company handles, and you'd never know it. In fact, the law forbids companies from disclosing that a request for information has been made. Consequently, no one is certain how much personal information is being requested. However, on Jan. 15, the Associated Press reported that the FBI is storing 257.5 million records on people who flew on commercial airlines between June and September 2001. "David Hardy, the FBI's chief of the record and information dissemination section of the records management division, said in a legal document dated Jan. 5 that the data was being stored and combined with other information from the Sept. 11 investigation," the Associated Press's Leslie Miller reported.

Such "other information" may very well include personal data about Canadian citizens handled on behalf of Canadian companies by U.S. firms. Last September, CIBC notified its Visa cardholders that their account and transaction records were open to scrutiny under U.S. law, since the bank uses a U.S.-based company to handle some processes. As of last Oct. 1, the Visa cardholder agreement was modified accordingly.

In today's global economy, however, a Canadian corporation could have trouble figuring out whether the information it handles is open to U.S. investigators. As is potentially the case for CIBC Visa, a U.S.-based firm that handles or processes data on behalf of a Canadian company is required to comply if it receives a demand for the information under the Patriot Act, and is forbidden from letting the Canadian company know about it. Such a case would apply equally whether the service provider was actually located in the U.S., or whether it was based there but working on Canadian soil. It even applies in the case of Canadian subsidiaries of U.S. firms. "You might have a recovery site in the United States. You may do backup and archiving through a network, and the network may choose where they have room to back up the net-



## Uncle Sam and you

DEBATE ABOUT THE U.S.A. PATRIOT ACT REPLAYS THE CLASSIC TUG-OF-WAR BETWEEN INDIVIDUAL FREEDOM AND PUBLIC SAFETY. FOR CANADIAN BUSINESSES, THE LEGISLATION RAISES SOME TRICKY QUESTIONS

work. It brings into question whether that information would be adequately protected while it's outside of Canada," says Robert G. Parker, a partner with Deloitte & Touche in Toronto. "Concerns have been raised over the planned processing of Canadian census information in the United States." (In these cases, standard security practices like data encryption offer some protection, but they won't help if anyone at the U.S. end of the operation has access.)

**WHAT BRITISH COLUMBIA DID** British Columbia's Government and Service Employees' Union vociferously raised concerns as early as 2003, when the provincial government

