SIDLEY AUSTIN BROWN & WOOD LLP
AND AFFILIATED PARTNERSHIPS

DECEMBER 22, 2003

PRIVACY AND DATA PROTECTION ALERT

Privacy, Data Protection and Information Security Practice Group

Sidley Austin Brown & Wood LLP offers clients an inter-disciplinary, international group of lawyers focusing on the complex issues of privacy, data protection, information security, consumer protection and cybercrimes. Members of the Privacy Group are based primarily in Washington, New York, London, Chicago, Brussels, Los Angeles, and San Francisco. The Group includes intellectual property lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, and regulatory and white collar lawyers.

If you would like more information on the Privacy, Data Protection and Information Security Practice Group, please contact:

Alan Charles Raul
202-736-8477
araul@sidley.com

To receive future copies of the Privacy and Data Protection Alert via email, please send your name, company or firm name and email address to lhersh@sidley.com

Stringent Canadian Privacy Law to Take Effect January 1, 2004

Alan Charles Raul*
Edward R. McNicholas
Jennifer Tatel

United States companies that conduct business in Canada, as well as most other organizations that collect, use or disclose personal information in the course of a commercial activity within Canada, may be subject to a new law providing expansive privacy protections for Canadian citizens. Effective January 1, 2004, such companies will have to comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA or the Canadian Privacy Law). The Canadian Privacy Law deserves particular attention because it entails more extensive privacy requirements than are generally applicable under United States law.

The new Canadian privacy regime is essentially a European-style approach to privacy. Under United States privacy laws, different sectors - medical, financial, communications - have different privacy rules, and many sectors face few statutory privacy rules. The Canadian Privacy Law, in contrast, is comprehensive and highly prescriptive. Every organization that collects, uses or discloses personal information in the course of a commercial activity is subject to the Canadian Privacy Law - from dress shops to furniture companies to mail-order houses.

Like the EU Data Protection Directive, the Canadian Privacy Law generally requires covered organizations to obtain the consent of an individual before collecting, using or disclosing his personal information.

* Sidley Austin Brown & Wood LLP has prepared this article for informational and educational purposes only. It does not constitute legal advice and is not a legal opinion regarding the law of either the United States or Canada. Mr. Raul, Mr. McNicholas, and Ms. Tatel are United States, not Canadian, attorneys. The article is not intended to create, and receipt of it does not create, an attorney-client relationship. Although Sidley has extensive experience addressing global privacy issues in consultation with local counsel as necessary, readers should consult Canadian counsel for definitive guidance and opinions regarding PIPEDA.

This personal information may be used only for the purpose for which it was collected; any further use usually requires the organization to obtain further consent from the individual. Even with consent, however, an organization may collect only that information that a "reasonable person" would consider appropriate under the circumstances.

The Canadian Privacy Law rests on an express concept of "reasonableness." This apparent flexibility, however, will not necessarily provide significant compliance benefits for covered organizations. Indeed, it may subject businesses to considerable uncertainty about what is required to comply. For example, the law does not specify the type of consent people must give - that is, whether they must opt-in or merely be allowed to opt-out. Instead, in determining the form of consent to use, organizations are required to take into account "the sensitivity of the information" and the "reasonable expectations of the individual." (§ 4.3.5). The Canadian scheme thus does not mandate (or bless) a specific form of consent. It instead requires consent that is effective in light of each collection, each particular use, and each particular disclosure. In the United States, the norm for consent is to provide an "opt-out" option for those who do not consent. Under the Canadian regime, "opt-out" consent may or may not be adequate depending upon whether the Canadian Privacy Commissioner deems it "reasonable" under the specific circumstances. The text of the Canadian Act appears to allow, in essence, a sliding scale from express opt-in consent to tacit opt-out consent based on the sensitivity of the information and the reasonable expectation of individuals. In the hands of reasonable regulators and enforcers, this flexible, "balancing" approach could be helpful. However, precisely where a particular set of data falls on the sensitivity scale will only become clear over time. The aggressiveness of Canadian privacy enforcement is also an evolving factor.

Another significant provision is that the Canadian Privacy Law requires notice retroactively for information already gathered. Thus, companies must analyze the personal information already in their possession and ensure compliance with the notification requirements of the Act.

As with the European regime, the Canadian law also mandates that customers must have access to their personal information and the ability to challenge or correct any misinformation possessed by the company. Furthermore, the law requires physical, technological, and organizational safeguards on information such as physical locks, passwords, and confidentiality agreements - all of which may create a font of liability for companies who suffer computer security breaches.

In contrast to the US privacy regime, which the EU has found "inadequate," the Canadian law is perceived so strict by the EU that it has been deemed to provide "an adequate level of protection." (The full text of the EU Decision, published in the EU Official Journal on Friday, January 4, 2002, is available at: http://europa.eu.int/eurlex/en/archive/2002/l_00220020104en.html). The upshot of this finding is that companies will be able to transfer data from the EU into Canada without the need for membership in the "Safe Harbor" or compliance with other mechanisms that are required for EU to US transfers. Accordingly, use of Canadian subsidiaries may be a solution for some international data transfer issues.

Enforcement under the Canadian Privacy Law is initially through consumer complaints to the organization which controls the data. Consumers may then

file a complaint with the Privacy Commissioner, who has jurisdiction to investigate complaints and publish opinions. The Privacy Commissioner may also take the complaint to the Federal Court of Canada. Alternatively, after a consumer has received the Privacy Commissioner's report, under certain circumstances, a direct private right of action exists in the Federal Court of Canada.

The Canadian Privacy Law previously went into effect for certain highly-regulated areas such as financial institutions and organizations that sell personal information across provincial or national borders, including organizations that lease, sell or exchange mailing lists. The January 2004 date brings the law into full effect for all organizations in every sector, except those with specific exemptions.

In a series of rulings since the Canadian Privacy Law became effective, the previous Privacy Commissioner of Canada demonstrated his intent to strictly enforce compliance with the law. Several major Canadian companies were subject to enforcement actions which required them to re-design privacy policies and marketing efforts and face the potential for significant damages. For instance, AirCanada was required to alter and re-distribute its privacy policy because the Privacy Commissioner decided that a different type of consent was required. For more information, see "Canada's Tough Enforcement of Its Privacy Regime May Affect United States Privacy Practices" (April 12, 2002) http://www.sidley.com/cyberlaw/features/canada.asp. Reflecting a potential change in emphasis, Canada's new Privacy Commissioner, who took over the position on December 1, 2003, has pledged that she will be "very sympathetic" to organizations' attempts to implement provisions of the Canadian Privacy Law.

For the present time, the complexity of privacy law in Canada appears only to be growing given that individual Canadian provinces are free to enact more strict privacy provisions. On December 3, 2003, the Canadian federal government largely exempted businesses and other organizations in the province of Quebec from the new federal privacy law because Quebec's 1994 "Act Respecting the Protection of Personal Information in the Private Sector" is substantially similar to the new federal Act. Accordingly, the existing provincial law will continue to apply. Moreover, the Canadian federal government has the authority to exempt other provinces that have their own privacy laws if they are substantially similar to the federal law, and the Privacy Commissioner must annually review such substantially similar laws. In addition, some jurisdictions within Canada have enacted special laws dealing with personal health information, and other laws, such as the federal Bank Act, contain privacy provisions.

United States organizations with business or customers in Canada or operating across the international border should review their existing privacy policies and practices to determine whether they may be subject to the Canadian privacy regime.

Please contact the following lawyers in the Privacy Group for more information:

Washington

Alan Charles Raul
202-736-8477
araul@sidley.com

Andrew J. Strenio
202-736-8614
astrenio@sidley.com

Michael F. McEneney
202-736-8368
mmceneney@sidley.com

Bradford A. Berenson
202-736-8971
bberenson@sidley.com

Frank R. Volpe
202-736-8366
fvolpe@sidley.com

Anita L. Wallgren
202-736-8468
awallgren@sidley.com

Edward R. McNicholas
202-736-8010
emcnicholas@sidley.com

New York

Peter J. Toren
212-839-7355
ptoren@sidley.com

Alan L. Jakimo
212-839-5480
ajakimo@sidley.com

Chicago

Jeffrey S. Rothstein
312-853-7260
jrothstein@sidley.com

Mark Kaufmann
312-853-2221
mkaufmann@sidley.com

Karen Owen Dunlop
312-853-2223
kdunlop@sidley.com

Laura J. Cole
312-853-7725
lcole@sidley.com

Los Angeles

Ron C. Ben-Yehuda
213-896-6668
rbenyehu@sidley.com

London

John M. Casanova
020 7360 3739
jcasanova@sidley.com

William R.M. Long
020 7778 1865
wlong@sidley.com

Susan L. Atkinson
020 7778 1869
satkinson@sidley.com

Brussels

Richard L.A. Weiner
32 2504 6450
rweiner@sidley.com

Maurits J.F. Lugard
32 2504 6400
mlugard@sidley.com

San Francisco

Philip Woo
415-772-7428
pwoo@sidley.com