WILMERHALE

Recent International Developments on Internet Privacy

2000-04-18

Two recent legal developments will significantly affect Internet companies' use of consumer information: (i) the proposed EU-U.S. Data Privacy Agreement, and (ii) Canada's Personal Information and Electronic Documents Act.

EU - U.S. Data Privacy Agreement

On March 14, 2000, nearly 18 months after the Directive on Data Protection (the "Privacy Directive") became effective, the European Union ("EU") and the United States announced a provisional agreement on the transfer of personal data from the EU to the United States. The agreement will affect U.S. companies collecting personal information about European consumers.

Background -- EU Privacy Directive

As previously discussed in our June 24, 1999 Internet Alert, the EU Privacy Directive took effect October 25, 1998, establishing a set of legal principles for privacy protection and the free flow of data within the fifteen-country EU. It prohibits transfers of personally identifiable information to non-EU countries unless "adequate" privacy standards are observed. As the Directive applies to personal data about EU nationals collected over the Internet by companies, no matter where those companies are located, it potentially applies to every e-commerce company or web site operator in the United States.

The United States has not enacted broad privacy protection laws, choosing to rely instead on a combination of narrowly-tailored federal privacy laws, state regulation, and private-sector "self-regulation." The Federal Trade Commission has also shown a willingness to investigate

and intervene in a variety of high-profile privacy-related cases. However, applying the standards from the Privacy Directive, this patchwork system of privacy regulation is unlikely to be deemed "adequate." Without the new agreement, transfers of personally identifiable information from the EU to the United States could have been prohibited.

Privacy Agreement

The proposed EU-U.S. Data Privacy Agreement creates voluntary "safe harbor" principles for the protection of personally identifiable information, based largely on widely-accepted privacy principles. If an organization decides to adhere to the safe harbors and complies with them, then it will qualify as a company offering "adequate" privacy protection for the purposes of the EU Privacy Directive, and thus will be eligible to transfer personal data from the EU to the United States.

The proposed safe harbor guidelines include seven privacy principles. These guidelines still await final approval, after considering and possibly incorporating comments received by the U.S. Department of Commerce.

1. NOTICE: Companies which collect personally identifiable information must state why the information is collected, provide a contact point for questions or complaints, disclose the types of third parties which will have access to the information, and state whether and how such access may be limited. The notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the requesting organization, or as soon thereafter as is practicable, but in any event before the organization: (i) uses such information for a purpose other than that for which it was originally collected or processed by such organization; or (ii) discloses it for the first time to a third party.
2. CHOICE: Individuals must be allowed to choose whether their information will be used (by the original collector of the information or by third parties) for purposes other than the purpose for which it was originally collected. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. For "sensitive" information relating to health, race, political opinions, ethnicity, religion, trade union membership, and sex, individuals must explicitly authorize ("opt in") such uses. For other personal data, an "opt out" procedure is sufficient. In practice, notwithstanding the possibility of using an "opt out" procedure for some personal data, it may be advisable to use the "opt in" procedure for all personal data. This choice is not required for uses which are "compatible" with the original purpose

for collecting the information.

3. ONWARD TRANSFER: So long as personal information is used for its original purpose, it may be transferred to a third party, provided the third party recipient also follows these safe harbor principles.
4. SECURITY: Organizations creating, maintaining, using or disseminating personal information must take "reasonable" precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.
5. DATA INTEGRITY: When personal data is processed, users must take "reasonable" steps to ensure that the data is reliable for its intended use, accurate, complete, and current.
6. ACCESS: Individuals must be allowed to access data about themselves in order to ensure its accuracy. This right, however, will not be absolute, and the obligation to provide access depends upon whether there will be a risk to the individual"s or other person's privacy, as well as the costs of providing access.
7. ENFORCEMENT: Individuals must be given an opportunity to pursue complaints and disputes involving the use or disclosure of their personal information. Among other things, the mechanisms to resolve disputes must be, at a minimum, "readily available and affordable."
8. Companies may provide enforcement mechanisms by (1) complying with private-sector self-regulatory programs, (2) complying with an applicable privacy law or regulation which provides for the handling of individual complaints and dispute resolution, or (3) committing to cooperate with EU data privacy protection authorities. (see full text version as of April 14, 2000).

The U.S. Commerce Department will keep a register of industry self-regulators and monitor those companies to ensure they comply with privacy rules. These self-regulatory authorities will have to reapply for membership on the list each year. Failure to comply with the safe harbor principles will be considered a deceptive business practice and a prosecutable offense in the EU. Publication of violations by the EU should also deter companies from breaking the law.

Outlook

The financial services industry is an important area where data protection arrangements have not yet been finalized, due to the changing legal situation in this sector in the United States. However, the EU and the United States hope to reach agreement on including financial services in a safe harbor arrangement as soon as possible.

The provisional agreement must still be approved by the European Commission, its 15 Member States and the European Parliament. Approval procedures in the United States also require widespread consultation, including the National Economic Council and other bodies. It is expected to go into effect in late June or July 2000. Companies will be reviewed in mid-2001 to see if they have complied with these privacy laws.

The agreement will help to avert a feared trade dispute over the tough EU standards embodied in the Privacy Directive. It will facilitate trans-Atlantic information flows by providing both legal certainty for operators and safeguards for consumers demanding protection of their privacy.

Changes to Canada's Privacy Law

Canada's new privacy legislation was passed by the House of Commons on April 4, 2000. Once it comes into force, it will have a significant impact on many Canadian companies and the operations of certain U.S. and other foreign companies doing business in Canada.

New Bill

The Personal Information and Electronic Documents Act, see Bill C-6 (previously Bill C-54), consists of several parts. Only Part 1 and Schedule 1 address personal information protection. Parts 2 to 5 address changes to government processes to enable greater use of electronic documents, establish evidentiary rules for electronic documents, and allow electronic publishing of official information.

Part 1 establishes rules for the protection of all personal information (i.e. information about identifiable individuals) that is collected, used and disclosed in the course of commercial activities in Canada. Organizations (defined to include associations, partnerships, individuals and trade unions) will generally be required to explain the purpose of collection, and obtain the consent of individuals to collect, use, and disclose such information. They will be expected to limit collection to necessary purposes and to adopt adequate safeguards to protect such information from disclosure. Individuals must be provided with reasonable access to their personal information, an opportunity to challenge the accuracy of such information and the right to have it amended, where appropriate. Organizations subject to the legislation will be made accountable for personal information which they collect, use, or disclose.

Individuals have a right to file complaints with Canada's Privacy Commissioner against

organizations for certain alleged violations of the legislation. The commission may investigate and attempt to resolve complaints. Certain complaints can be taken to the Canadian Federal Court for resolution. The bill allows for penalties and punitive damages, with no limit set on such damages.

Outlook

The Personal Information and Electronic Documents Act is not expected to come into force until January 2001. This delayed effective date is intended to provide organizations with the necessary lead-time to become compliant with the new legislation.

Once in force, the legislation will initially apply to organizations operating in federally regulated industries, such as transport, communications, banking, shipping and the airlines, as well as to organizations in respect of the collection, use or disclosure of personal information which crosses provincial boundaries. Unless provinces adopt comparable laws within a three year period, the bill will also be made applicable to organizations with commercial activities in respect of personal information collected, used or disclosed solely within a province.

According to the Privacy Commissioner of Canada, the new Canadian legislation would help Canada meet new data protection standards set by the EU Privacy Directive. Currently, Quebec is the only jurisdiction in North America with a private sector data protection law that meets the requirements imposed by the EU Privacy Directive.

Safe harbors will not have to be created through any EU-Canadian negotiated agreement, for Canadian companies will be required by law to meet standards consistent with the data protection standards in the EU Privacy Directive. Canada will thus be considered a non-EU country where "adequate" privacy standards are observed, so transfers of personally-identifiable information from the EU to Canada will be allowed to continue.

As with the EU-U.S. Privacy Agreement, the new Canadian legislation should promote electronic commerce by protecting personal information. Furthermore, parts 2 to 5 of the legislation will ensure that e-commerce transactions have the same legal standing as paper transactions, and will provide for the recognition of electronic signatures.

There will probably not be the need for any diplomatic discussions between the United States and Canada as a result of this legislation. Unlike the EU Privacy Directive, there is no bar in the Canadian legislation on data transfers to countries with lower privacy standards. However,

U.S. companies subject to Canadian jurisdiction will still need to comply with this new legislation, to the extent that it applies to their collection, use and disclosure of personal information of Canadian nationals.

Barry Hurewitz

barry.hurewitz@haledorr.com