

Privacy Newsletter

JUNE 2002

www.mintz.com

PRIVACY NEWS

Domestic Developments

Minnesota Governor Jesse Ventura has signed into law a bill that permits users to limit the use of data collected by Internet Service Providers (ISPs) (S.F. 2908). The bill requires ISPs to obtain users' consent before revealing their personal information or browsing history, and permits aggrieved individuals to enforce their rights through private law suits. The bill also restricts the transmission of unsolicited commercial e-mail. Critics of the bill warn that it will hamper law enforcement investigations of cyber-crime. Critics also argue that the law provides only marginal privacy protection because it applies to ISP's, but not commercial Web site operators that collect a variety of personal information from visitors.

The Senate Commerce Committee has approved bills to regulate consumer privacy online and restrict the transmission of spam. The Committee approved Senator Hollings's Online Personal Privacy Act (S. 2201) despite some concern that its failure to regulate offline data collectors unfairly discriminates against the online services industry. The Committee also approved Senator Burns's CAN SPAM Act that would require initiators of unsolicited e-mail messages to provide an opportunity for recipients to opt out of future communications and create criminal penalties for the falsification of origination addresses.

International Developments

Europe • The European Commission (EC) has launched an investigation into whether Microsoft's .NET Passport system violates European Union (EU) data privacy laws. The Commission claims that Microsoft did not inform EU authorities that the .NET Passport system collects information from consumers making online purchases. Although Microsoft has certified compliance to the safe harbor principles promulgated by the Department of Commerce in conjunction with the EU, the EC's actions indicate that the EC may seek to assert jurisdiction over Microsoft for the collection and use of personal information within the EU.

(continued on page 2)

FTC Issues Rule for Safeguarding Customer Information

Financial institutions under the Federal Trade Commission's (FTC's) jurisdiction have until May 23, 2003 to comply with the agency's final rule for safeguarding customer information. The Safeguards Rule requires each financial institution to develop an internal, written information security program that is appropriate to its size and complexity, the nature of its activities, and the sensitivity of the information at issue. Financial institutions subject to the Safeguards Rule are already obligated to comply with the privacy notice requirements set forth in the FTC's Privacy Rule, which went into effect on July 1, 2001. The Safeguards Rule does not affect the Privacy Rule's notice obligations, and does not obligate financial institutions to disclose their information security programs to customers.

The Safeguards Rule requires financial institutions to develop, implement, and maintain reasonable administrative, technical, and physical safeguards for the protection of customer information. The information security program must protect against anticipated threats or security hazards and unauthorized use that could result in substantial harm or inconvenience to any customer. The Safeguards Rule extends the security program obligations to affiliates of a financial institution, even though the companion Privacy Rule does not regulate information-sharing between financial institutions and affiliates. The FTC reasons that failure to extend the security requirement to affiliates would undermine any security program put in place by the financial institution.

In implementing the required information security program, financial institutions must designate an employee to coordinate the program and conduct a comprehensive risk assessment. The risk assessment should identify reasonably foreseeable internal and external risks to the security of customer information. At a minimum, the risk assessment should consider the risks in operational areas including employee training and management; information systems (including network and software design, information processing, storage, transmission, and disposal); and detecting, preventing, and responding to attacks, intrusions, and system failures.

The Safeguards Rule requires financial institutions to regularly test or monitor the effectiveness of key aspects of their information security programs and make necessary adjustments based on the results. Financial institutions must also adjust their programs in response to material operational changes or any other circumstances that they have reason to know will materially impact their programs.

(continued on page 2)

MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC

FTC Issues Rule for Safeguarding Customer Information (continued from page 1)

Finally, the Safeguards Rule requires financial institutions to contractually bind third-party service providers to implement and maintain the appropriate safeguards for customer information. Indeed, financial institutions must take “reasonable steps” to select third-party service providers capable of maintaining these safeguards. Financial institutions have until May 24, 2004, to bring service contracts in place by June 24, 2002, into compliance. Oddly, service contracts entered into after June 24, 2002, must prospectively address safeguarding of customer information, even though the obligations do not take effect until May 23, 2003.

The FTC’s Safeguards Rule applies only to financial institutions under the FTC’s jurisdiction and does not apply to financial institutions regulated by the banking agencies or the Securities and Exchange Commission. These agencies have already issued safeguard standards for the entities under their respective jurisdictions. ○

Privacy News (continued from page 1)

Europe • The European Parliament (EP) has approved a new data directive for the telecommunications industry that allows member states to authorize ISP’s and telecommunications service providers to retain customer data for law enforcement purposes. Civil libertarian groups staunchly oppose the new measure, arguing that data should be retained only as long as necessary to serve the purposes for which it is collected. The directive also bans unsolicited commercial e-mail except in limited cases where the sender has a pre-existing business relationship with the recipient and the message promotes a “similar category” of products. The directive requires Web site operators to provide visitors with notice and the opportunity to opt out of Web site tracking activities, but does not require prior consent for the use of cookies.

Canada • Ontario’s proposed Privacy of Personal Information Act makes opt in, rather than opt out, the standard for the collection, use, and disclosure of personal information. Proponents of the proposal argue that it reflects the growing trend in favor of express, rather than implied, consent regimes. ○

Mintz Levin and ML Strategies provide legal, legislative and consulting expertise on privacy as it relates to many issues. If you would like further information, please contact the Mintz Levin attorney who regularly handles your legal affairs, or one of the attorneys or senior professionals listed below.

Privacy Regulation

Neil H. Aronson.....	617 348 1809
Franklin Blackstone III	703 464 8144
Amy L. Bushyeager	202 434 7479
Gordon R. Caplan	212 692 6702
John M. Delehanty.....	212 692 6703
Robert Duggan	617 348 1780
Christopher J. Harvie.....	202 434 7377
Paul A. Hughes	203 787 6320
Julie E. Korostoff	617 348 1638
Fernando R. Laguarda	202 434 7347
Cynthia J. Larose	617 348 1732
Frank J. Marco.....	203 787 6310
Bruce D. Sokler	202 434 7303
Howard J. Symons	202 434 7305
Ivan S. Wool.....	212 692 6757
Wayne M. Zell	703 464 8135

Health Privacy

Michael D. Bell	202 434 7481
Linda D. Bentley	617 348 1784
Susan W. Berson	202 661 8715/212 692 6750
Raymond D. Cotton.....	202 434 7322
Erin Lewis Darling.....	202 434 7478
Hope S. Foster	202 661 8758
Ellen L. Janos.....	617 348 1662
Peter M. Kazon	202 661 8739
Rebecca A. Matthews.....	203 787 6329
Laura J. Oberbroeckling	202 434 7333
Eric S. Tower	202 434 7344

Privacy Litigation

Susan L. Burke.....	202 661 8707
Michael S. Gardener.....	617 348 1642
Kevin M. McGinty	617 348 1688
Laurence A. Schoen	617 348 1764

Employment Privacy

Jennifer B. Rubin.....	203 787 6324
------------------------	--------------

Legislative Privacy Strategies

David J. Leiter	202 434 7346
-----------------------	--------------

Public Relations Strategies

Jason D. Glashow	617 348 1667
------------------------	--------------

MINTZ LEVIN
COHN FERRIS
GLOVSKY AND
POPEO PC

One Financial Center
Boston, Massachusetts 02111
617 542 6000
617 542 2241 fax

11911 Freedom Drive
Reston, Virginia 20190
703 464 4800
703 464 4895 fax

157 Church Street
New Haven, Connecticut 06510
203 777 8200
203 777 7111 fax

ML
STRATEGIES

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
202 434 7300
202 434 7400 fax

666 Third Avenue
New York, New York 10017
212 935 3000
212 983 3115 fax