HB

273

# Representative Beth Kerttula

Alaska State Legislature, District 3
State Capitol • Juneau, Alaska 99801-1182 • (907) 465-4766 • Fax (907) 465-4748
E-mail: Representative_Beth_Kerttula@legis.state.ak.us • http://www.kerttula.net


# Memorandum

**Date:** April 11, 2000

**To:** Lesil McGuire, Aide
House Judiciary Committee

**From:** Gretchen Kaiser

**Re:** **HB 273: Internet Privacy for Alaskan Consumers**

---

Attached is a bill packet for CSHB 273 (L&C):

- A blank CS for CSHB 273 (L&C) version "K" which cleans up the previous version and addresses some concerns raised by Internet service providers.
- Sponsor Sta ement.
- Sectional Analysis that accompanies version "K".
- March 2, 2000 legal analysis from the Department of Law.
- March 17, 2000 fiscal note from Department of Law.
- Letters from Chugach Electric Association, Inc. (3/24/00), GCI (3/28/00), and Alaska Civil Liberties Union (3/24/00).
- CS HB 273 (L&C) – version "I".
- March 20, 2000 cover article on Internet privacy.

1-LS1156\K
Bannister
4/11/00

**CS FOR HOUSE BILL NO. 273( )**

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIRST LEGISLATURE - SECOND SESSION

**BY**

**Offered:**
**Referred:**

**Sponsor(s): REPRESENTATIVES KERTTULA, Dyson**

**A BILL**

**FOR AN ACT ENTITLED**

**"An Act relating to the disclosure of subscriber information by Internet service providers."**

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:**

* **Section 1.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(43) violating AS 45.50.479 (disclosure of information by Internet service provider).

* **Sec. 2.** AS 45.50 is amended by adding a new section to read:

**Sec. 45.50.479. Disclosure of information by Internet service provider.** (a) Except as provided in (b) or (c) of this section, an Internet service provider or an employee of an Internet service provider may not disclose subscriber information about a subscriber of the Internet service provider, or about another person who uses the provided Internet access services, to a third party for any purpose, including marketing, without the affirmative consent of the subscriber.

(b) An Internet service provider may disclose subscriber information without

the affirmative consent of the subscriber to an agency of the state, the federal government, or a municipality for the investigation of a criminal offense or an investigation related to a civil or administrative proceeding if, with regard to an investigation

(1) of a criminal offense, a court, upon application of the agency seeking information that is relevant to the investigation, has issued an order authorizing the disclosure of the subscriber information without the affirmative consent of the subscriber; or

(2) related to a civil or administrative proceeding, the agency makes a written request to the Internet service provider to disclose the subscriber information.

(c) An Internet service provider may exchange with other Internet service providers subscriber information necessary to maintain the proper functioning or integrity of the provider's network.

(d) When an Internet service provider activates a new account for a subscriber, the Internet service provider shall provide the subscriber by regular or electronic mail addressed to the subscriber's address and to the subscriber's personal attention with

(1) a description of the information on the subscriber that is generally available without restriction to users of the Internet;

(2) a statement indicating whether or not the subscriber has given affirmative consent to disclose subscriber information;

(3) a statement of the Internet service provider's policies that govern the subscriber information that may be disclosed with the subscriber's affirmative consent and a description of the subscriber information that will not be disclosed without the subscriber's affirmative consent;

(4) a statement that subscriber information will not be disclosed without the subscriber's affirmative consent except for

(A) exchange of subscriber information with another Internet service provider as necessary to maintain the proper functioning or integrity of the network of the subscriber's provider; or

(B) a disclosure of subscriber information to an agency of the state, the federal government, or a municipality for the investigation of a

criminal offense or an investigation related to a civil or administrative proceeding under (b) of this section;

(5) a statement of the provider's policies governing disclosure under (4) of this subsection; and

(6) a statement of the circumstances under which the network administrator or network contractor of the Internet service provider is permitted to review the contents of the subscriber's electronic mail or web site traffic; in this paragraph, "network contractor" means the person or entity paid directly by the Internet service provider to supply and maintain bandwidth, server space, and network support software.

(e) Notwithstanding AS 45.50.531(a), if an Internet service provider or an employee of the Internet service provider discloses subscriber information in violation of this section, the subscriber, or the state on the subscriber's behalf, may bring a civil action against the Internet service provider to recover $500 as damages for each disclosure. Each item of subscriber information that is disclosed is considered a separate disclosure for which $500 may be awarded as damages. The $500 award constitutes the value under this subsection of damages for the violation, and the subscriber or the state is not required to prove actual damages. An action under this subsection is in addition to any other remedy allowed under AS 45.50.471 - 45.50.561.

(f) This section does not apply to disclosure of subscriber information by an Internet service provider if the application of it would violate 15 U.S.C. 6502(d) (Children's Online Privacy Protection Act of 1998).

(g) In this section,

(1) "affirmative consent" means a statement in electronic form or a written statement on paper from a subscriber authorizing an Internet service provider to distribute personal subscriber information to third parties for marketing or other purposes;

(2) "criminal offense" has the meaning given to "offense" in AS 11.81.900(b);

(3) "direct Internet access services" means direct transmission control protocol/Internet protocol (TCP/IP) services if the services

(A) include access to a domain name server and an electronic mail server; and

(B) are provided by dial-up modem connections using a telephone, the Integrated Services Digital Network, a digital subscriber line, or a coaxial cable, or by other means;

(4) "Internet service provider" means a person that engages in the business of providing direct Internet access services to other persons;

(5) "subscriber" means a person who contracts with an Internet service provider to receive direct Internet access services if the person's address provided to the Internet service provider is located in this state;

(6) "subscriber information" means information obtained from or as a result of the contract between an Internet service provider and a subscriber; the term

(A) includes

(i) social security number, date of birth, occupation, credit card information, debit card information, current address, prior addresses, telephone number, mother's maiden name, and income information; and

(ii) information gathered by means of tracking Internet usage, Internet protocol connection history, Internet preferences, computer equipment, computer software, or subscriber profiles;

(B) does not include the subscriber's name, the subscriber's electronic mail address, and aggregated data that cannot be used to identify a subscriber;

(7) "third party"

(A) means a person who is not the Internet service provider, an employee of the Internet service provider, or the subscriber;

(B) includes an entity that controls, is controlled by, or is under common control with the Internet service provider.

* **Sec. 3.** The uncodified law of the State of Alaska is amended by adding a new section to read:

APPLICABILITY. AS 45.50.479, enacted by sec. 2 of this Act, applies to contracts

between Internet service providers and subscribers if the contracts are in existence when this Act takes effect or are entered into on or after the effective date of this Act. In this section, "Internet service provider" and "subscriber" have the meanings given in AS 45.50.479(g).

*** Sec. 4.** The uncodified law of the State of Alaska is amended by adding a new section to read:

TRANSITIONAL PROVISION. In addition to providing information under AS 45.50.479(d), added by sec. 2 of this Act, to subscribers with new accounts, an Internet service provider shall also, under AS 45.50.479(d), provide the information required by that subsection in the manner required by that subsection to the provider's subscribers who entered into contracts with the provider before the effective date of this Act and whose contracts are in existence on the effective date of this Act. In this section, "Internet service provider" and "subscriber" have the meanings given in AS 45.50.479(g), added by sec. 2 of this Act.

**Representative Beth Kerttula**

**Sponsor Statement**

# CS HB 273
# Internet Privacy for Alaskan Consumers

In the past few years, Alaskans have eagerly embraced Internet service into their homes and businesses. Access to the World Wide Web enables Alaskans to overcome geographic remoteness and time differences and to interact globally for ideas, information, and business. However, technological advances and business practices in the rapidly evolving electronic world have the potential for unprecedented access to Internet consumers' personal information and their on-line usage and preferences. Building upon the Alaska Constitution's strong foundation of Alaskans' right to privacy, CSHB 273 updates our consumer protection laws to address Internet activity.

CSHB 273 takes an important first step to protect Alaskan consumers' privacy at their entry point to the World Wide Web – their Internet service provider. CSHB 273 prevents an Internet service provider and its employees from disclosing a subscriber's personal identification information and any data that records a subscriber's Internet use or preferences *unless the subscriber agrees to the use of their information.* Family, friends, or employees using the subscriber's Internet account are also protected. CSHB 273 makes exceptions for disclosure of information in a law enforcement investigation or in order to maintain the proper functioning and integrity of the Internet service provider's network. As with other violations of Alaska consumer protection laws, CSHB 273 provides for civil penalties.

CSHB 273 protects a subscriber whose address is located in this state. It focuses solely on the subscriber's contractual relationship with an Internet service provider and does not address consumer privacy at the "other end" as Alaskans visit the virtually limitless web sites. The U.S. Federal Communications Commission and Federal Trade Commission, U.S. Congress, international organizations, and Internet business alliances are wrestling with these interstate and global privacy issues. CSHB 273 also does not legislate Internet content, minors' access to adult sites, or the collection of taxes on Internet sales.

CSHB 273 protects Alaskans' privacy by helping individuals maintain control over use of their personal information as they access the Internet.

# Internet Privacy for Alaskan Consumers
# CS House Bill 273
# ("K" Version)

## Sectional Analysis
(Updated 4/11/00)

**SECTION 1.** Paragraph AS 45.50.471(b)(43) adds disclosure of information by an Internet service provider (ISP) to the list of unlawful acts and practices.

**SECTION 2** Section AS 45.50.479 places limitations on an Internet service provider's use of a subscriber's personal information.

subsection (a) – prohibits an ISP or their employee from disclosing a subscriber's information unless the subscriber gives consent. The subscriber is protected without taking action; the burden is on the ISP to obtain consent. Other users of the subscriber's Internet account (such as a family members) are also protected.

The section may raise a legal issue since regulating Internet service providers who operate outside Alaska places some burden on interstate commerce. The attached March 2, 2000 Department of Law analysis of this issue concludes that

> "Any *burden proposed AS 45.50.479 may impose on interstate commerce is likely to be seen as incidental when balanced against the legitimate government interest in protecting consumers from unwarranted intrusions upon their privacy and insuring that consumers are protected against abusive and unwarranted disclosure practices.*"

Also, Theresa Bannister, Legislative Counsel, noted in her 11/15/99 memorandum accompanying a work draft of HB 273 that

> "*It is likely that individual privacy rights would be considered very valuable. The burdens on the interstate providers do not, at least on the surface, appear to be very onerous.*"

subsection (b) – permits an ISP to disclose subscriber information in a law enforcement investigation, and clarifies ISP disclosure for civil and criminal investigations.

**New:** subsection (c) – permits an ISP to exchange information with other ISPs to protect the integrity of the provider's network in the event of a hacker's attack. This responds to a concern raised by GCI, in its March 28, 2000 letter, regarding the ability of Internet service providers to work together to counter Internet abusers.

**Amended:**

subsection (d) – identifies information that the ISP must provide in a notice to a new subscriber. The ISP would be required to describe how the subscriber's information would or would not be disclosed. The notification language, which was added from HB 410 in (H) L&C Committee, is clarified and simplified in this version.

For example, a subscriber might agreed that his or her information could be disclosed to an outside vendor providing filtering service for the ISP (e.g., a service purchased by parents to block certain adult sites for underage Internet users). In this case, the ISP notice would describe, under subsection (d)(3), what information would be disclosed. Similarly, GCI's March 28, 2000 letter describes the need to share subscriber information between a ISP wholesaler and ISP retailer. CS HB 273 allows this to happen once the ISP obtains subscriber consent and describes to the subscriber what information would be shared.

subsection (e) - establishes a civil penalty for disclosure of subscriber information. The penalty is set at $500, similar to the other unlawful acts governed by this statute. However, the Internet subscriber is not required to prove actual damages as in AS 45.50.531, since it would be subjective and difficult, at best, to place a monetary value on the loss of personal information and one's privacy. Other legal remedies, such as action by the state attorney general, are also allowed.

subsection (f) – recognizes federal Children's Online Privacy Protection Act limitation on disclosure of information about or by children under 13.

subsection (g) – provides several definitions, including:

**Amended:** "affirmative consent" is a *statement in electronic form* or a written statement providing consent by the subscriber. Adding consent via an electronic format responds to a March 24, 2000 letter from Chugach Electric Assn., Inc.

"subscriber" is a person (i.e., individual or business) with an in-state address;

**Amended:** "subscriber information" is both personal identifying information *and* records of a subscriber's pattern of Internet use. Language is added to make clear that a subscriber's name and email address is *not* included under this definition. A subscriber's name and email address is generally available on the Internet.

**Amended:** "third party" is amended at (B) to substitute "entity" for "organization" and generally has the meaning of an affiliate of an ISP. This responds to a comment from Chugach Electric Assn. in its March 24, 2000 letter.

**SECTION 3** Applies AS 45.40.479 to new and existing contracts between Internet service providers and subscribers. The application of this bill to contracts entered into prior to the effective date of this Act may raise an issue under state and federal prohibitions against state impairment of existing contracts. The issue depends on:

- whether the subscriber information is an essential part of a contract with valuable results to the ISP;
- whether the consumers have been aware that their information is being used; and
- if the proposed restriction cures a significant privacy problem.

The attached Department of Law 3/2/00 analysis addresses this issue. At this point, there is no information that would lead to the conclusion that the bill would impair existing contracts. If ISPs consider subscriber information to be highly valuable and marketable, then the Alaskan consumers' personal data and Internet patterns are most likely being used and HB 273 would overcome a significant consumer privacy problem.

**NEW: SECTION 4** – describes a transition so that an ISP provides notification under AS 45.50.479(d) to existing subscribers about the disclosure of each subscriber's information. The bill does not currently establish a deadline for this notification of existing subscribers.

# STATE OF ALASKA

*TONY KNOWLES, GOVERNOR*

**DEPARTMENT OF LAW**

*OFFICE OF THE ATTORNEY GENERAL*

*1031 WEST 4TH AVENUE, SUITE 200*
*ANCHORAGE, ALASKA 99501-5903*
*PHONE: (907)269-5100*
*FAX: (907)276-3697*

March 2, 2000

The Honorable Beth Kerttula
House of Representatives
State Capitol
Juneau, AK 99801-1182

Re: HB 273
Internet Privacy for Alaskan Consumers

Dear Representative Kerttula:

Here is the analysis you recently requested regarding the Commerce Clause and Contract Impairment issues relating to HB 273, the Internet Privacy for Alaskan Consumers bill.

## I. Commerce Clause Analysis

### A. Question presented.

You have posed the following question to the Department of Law:

> "*The U.S. Constitution_Commerce Clause and regulation of Internet service providers.* Does HB create an issue by imposing an excessive burden on interstate commerce, compared with the likely valuable individual privacy benefits?"

### B. Short Answer.

Any burden proposed AS 45.50.479 may impose on interstate commerce is likely to be seen as incidental when balanced against the legitimate government interest in protecting consumers from unwarranted intrusions upon their privacy and insuring that consumers are protected against abusive and unwarranted disclosure practices.

C. **Analysis.**

Proposed AS 45.50.479 raises the question of whether prohibiting out-of-state Internet service providers from disclosing subscriber information to a third party discriminates on the basis of interstate commerce, thereby violating the Commerce Clause of the United States Constitution. States retain authority to exercise police powers to control matters of local concern even though interstate commerce may be affected. Maine v. Taylor, 477 U.S. 131, 133, 106 S.Ct. 2440, 91 L.Ed.2d 110 (1986). Courts apply a two-tiered analytical approach to Commerce Clause challenges. Brown-Forman Distillers Corp. v. New York Liquor Authority, 476 U.S. 573, 579, 106 S.Ct. 2080, 90 L.Ed.2d 552 (1986); Dayhoff v. Temsco Helicopters, Inc., 848 P.2d 1367, 1370-71 (Alaska 1993). If the practical effect of the statute is to discriminate or directly regulate interstate commerce, courts typically strike down the statute as invalid without further inquiry. Id. at 1370, n. 1.

Conversely, if the statute only indirectly impacts on interstate commerce and does not discriminate, courts apply the balancing test articulated in Pike v. Bruce Church, Inc., 397 U.S. 137, 142, 90 S.Ct. 844, 25 L.Ed.2d 174 (1970), wherein the court must determine (a) whether the statute effectuates a legitimate local interest, and (b) "whether the burden on interstate commerce clearly exceeds the local benefits." Brown-Forman, 476 U.S. at 579; Pike, 397 U.S. at 142.

A court would likely apply the Pike balancing test in evaluating proposed AS 45.50.479's effect on interstate commerce, because proposed AS 45.50.479's terms apply equally to both in-state and out-of-state Internet service providers. In applying the Pike test, any burden proposed AS 45.50.479 may impose on interstate commerce is likely to be seen as incidental when balanced against the legitimate government interest in protecting consumers from unwarranted intrusions upon their privacy and insuring that consumers are protected against abusive and unwarranted disclosure practices. Therefore, proposed AS 45.50.479 does not "clearly exceed" the local interests promoted by the bill. Brown-Forman, 476 U.S. at 579; Pike, 397 U.S. at 142.

## II. **Contract Impairment analysis**

A. **Question presented.**

You have also posed the following question to the Department of Law:

> "*Contract Impairment issue*. HB 273 would apply the requirements to existing subscriber contracts. Does this provision raise an issue under the state and federal prohibitions against state impairment of contracts?"

B. **Short Answer.**

A court would likely determine that proposed AS 45.50.479 does not substantially impair an Internet service provider's rights under existing contracts, and would therefore uphold the validity of the legislation in the face of an Impairment of Contract challenge.

C. **Analysis.**

Proposed AS 45.50.479 raises the question of whether an Internet service provider's rights under existing contracts (as opposed to contracts not yet entered into) with subscribers would substantially impaired in violation of the Contract Clause of the U.S. Constitution.

The Contract Clause prohibits states from enacting any law that retroactively impairs contract rights. (It does not affect contracts not yet entered into.) The Contract Clause prevents only substantial impairments of contract (i.e., destruction of most or all of a party's rights under a contract.) Moreover, not all substantial impairments are invalid.

In determining whether HB 273 is valid under the Contract Clause, a court would employ the following two-part test:

(1) Does the legislation substantially impair an Internet service provider's (or subscriber's) rights under existing contracts? If it does not, the legislation is valid under the Contract Clause. I would argue that the legislation only incidentally affects an Internet Service Provider's rights under existing contracts with subscribers, since the main purpose of such contracts is to provide the subscriber with Internet access in return for a fee. The Internet service provider's right under existing contracts to disclose subscriber information to a third party is only ancillary to the main purpose of the contract with a subscriber, and therefore prohibiting such disclosure through state legislation does not constitute a substantial impairment under a Contract Clause analysis.

(2) If the legislation were to be considered a substantial impairment of contract rights, the legislation would only be valid if it:

(a) serves an important and legitimate public interest; (I would argue that HB 273 certainly accomplishes an important and legitimate public interest in protecting subscribers from unwarranted intrusions upon their privacy and insuring that subscribers are protected against abusive and unwarranted disclosure practices.); and

(b) is a reasonable and narrowly tailored means of promoting that interest; (again, I would argue that HB 273 satisfies this test as well).

HB 273 should, in all likelihood, survive a Contract Clause challenge. Its restrictions on existing contract rights are minor compared to other instances in which Impairment of Contract challenges to state statutes failed. Here are three examples of cases in which state statutes survived Contract Clause challenges:

(1) Home Building & Loan Association v. Blaisdell, 290 U.S. 398 (1934): A Minnesota statute that imposed a moratorium on mortgage foreclosures during a severe depression did not violate the Contract Clause;

(2) Energy Reserves Group, Inc. v. Kansas Power & Light Co., 459 U.S. 815 (1983): A state statute placing a ceiling on price increases that a natural gas supplier could charge a public utility under the "escalator clause" of a preexisting contract did not violate the Contract Clause; and

(3) Keystone Bituminous Coal Association v. DeBenedictis, 480 U.S. 470 (1987): A state statute that restricted underground coal mining to protect a variety of public and private uses of surface land (and buildings) and that left the owners of subsurface mining rights with some reasonable value in, and return from, their investment did not violate the Contract Clause.

Very truly yours,

BRUCE M. BOTELHO
ATTORNEY GENERAL

By: Daveed A. Schwartz
Daveed A. Schwartz
Assistant Attorney General

DAS:jem

cc: Chrystal Smith
Legislative Liaison
Alaska Department of Law

# FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. HB 273

Revision Date/Time (Note if correction) _____ Dept. Affected Law
Title "An Act relating to the disclosure of subscriber information by Internet service providers." BRU Civil Division
Component Fair Business Practices
Sponsor Representative Kerttula
Requester House Labor and Commerce Committee Component No. 2206

**Expenditures/Revenues** (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

| OPERATING EXPENDITURES | FY 2001 | FY 2002 | FY 2003 | FY 2004 | FY 2005 | FY 2006 |
|---|---|---|---|---|---|---|
| Personal Services | | | | | | |
| Travel | | | | | | |
| Contractual | | | | | | |
| Supplies | | | | | | |
| Equipment | | | | | | |
| Land & Structures | | | | | | |
| Grants & Claims | | | | | | |
| Miscellaneous | | | | | | |
| TOTAL OPERATING | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| CAPITAL EXPENDITURES | | | | | | |
| CHANGE IN REVENUES ( ) | | | | | | |

**FUND SOURCE** (Thousands of Dollars)

| | | | | | | |
|---|---|---|---|---|---|---|
| 1002 Federal Receipts | | | | | | |
| 1003 GF Match | | | | | | |
| 1004 GF | | | | | | |
| 1005 GF/Program Receipts | | | | | | |
| 1037 GF/Mental Health | | | | | | |
| Other (Specify Type) | | | | | | |
| TOTAL | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |

**Estimate of any current year (FY2000) cost:** _____

**POSITIONS**

| | | | | | | |
|---|---|---|---|---|---|---|
| Full-time | | | | | | |
| Part-time | | | | | | |
| Temporary | | | | | | |

**ANALYSIS:** *(Attach a separate page if necessary)*

HB 273 adds to the Unfair Trade Practices and Consumer Protection Act disclosure of information about a subscriber, or other user of provided Internet access services, by the Internet service provider to a third party without the subscriber's permission. This prohibition would not apply to disclosure of such information to law enforcement in the course of an investigation. The subscriber could bring a civil action against the Internet service provider for violation of this section.

This bill is not anticipated to have a fiscal impact on the Department of Law.

Prepared by: Joan M. Kasson Phone 465-5370
Division Attorney General's Office Date/Time 3/17/00, 3:08 PM
Approved by Commissioner Bruce M. Botelho, Attorney General Date 3/17/00
Agency Department of Law

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**
For further distribution information, call the Governor's Legislative Office

(Rev 10/99) 2000/forms.xls/OMB

CHUGACH ELECTRIC
ASSOCIATION, INC.

EUGENE N. BJORNSTAD, P.E.
General Manager

March 24, 2000

Representative Beth Kerttula
State Capitol, Room 430
Mail Stop 3101
Juneau, Alaska 99801-1182

Re: HB 273

Dear Representative Kerttula:

Chugach Electric Association, Inc. is sympathetic with the needs of its customers to have information safeguarded. Chugach has always taken care to use the information our members entrust to us responsibly. Nevertheless, Chugach opposes HB 273 as currently drafted.

Chugach provides its customers with both electric service and, as an optional service, dial-up internet access services. Increasingly, customers like to purchase services such as dial-up internet service bundled with other services in different ways to suit their individual needs. Indeed, because customers want it, this is a prominent marketing strategy for utility service providers at this time. This bill interposes a major impediment to meeting customer needs in this way by preventing organizations which jointly market services from sharing customer information easily and efficiently. The bill seems designed specifically to prevent essential information sharing among joint marketers, subsidiaries or affiliates. Chugach believes that any benefit to customers is outweighed by the impediment to meeting customer needs.

This bill unfairly targets internet service providers as businesses which are prevented from sharing information while leaving all the many other businesses which routinely share information free to do so. Note that most of the information ISP's are prevented from disclosing is the same information routinely kept by other businesses and shared without these restrictions. If the bill embodies good rules for protecting customer information, those rules should be equally good for all businesses.

5601 Minnesota Drive • P.O. Box 196300 • Anchorage, Alaska 99519-6300
Phone 907-563-7494 • FAX 907-562-0027

The requirement that authorization to disclose information be written is particularly troublesome and anachronistic in this age of electronic communication and record keeping. Methods exist and are being developed which would allow customers to consent via electronic communication which would be adequate for demonstrating full consent but which would not involve the additional expense of maintaining written records.

The definition of "third party" is somewhat vague in part (B). It is not clear what would constitute an "organization" for these purposes.

Sincerely,

Eugene N. Bjornstad

Eugene N. Bjornstad
General Manager

cc: House Labor and Commerce Committee

March 28, 2000

Representative Fred Dyson
State Capitol
Juneau, AK 99801-1182

Representative Beth Kertulla
State Capitol
Juneau, AK 99801-1182

**RE: HB 273 relating to subscriber information**

Dear Representatives Dyson and Kertulla:

As one of the largest Internet Service Providers in Alaska, GCI is extremely concerned about the security of the Internet and the privacy of our customers. For those reasons, we applaud your interest in these matters. However, as presently drafted, HB 273 would severely limit our ability to preserve system integrity and protect our system, and customers, for various sorts of "cyber-attacks."

We have 2 persons on staff devoted to protecting the security of our system. Other local ISPs have similar staff. Our collective ability to protect the system, and to protect the vast majority of users from a small number of abusers, requires ISPs to coordinate security efforts. Today, a "security council" of ISPs and law enforcement personnel meet regularly in Anchorage to discuss and address security issues. All of these efforts require ISPs to share information in a manner which would be precluded by the legislation as drafted.

As a simple example, GCI and its subscribers could experience a "spam attack". Our security staff would attempt to track the source of the attack, which could lead to another ISP, such as Internet Alaska. Our staff would then contact Internet Alaska and would need to disclose certain "subscriber information." Of course, it is possible that a hacker may have "hijacked" another computer to distribute the spam, requiring further research and sharing of user information. These activities would be precluded by the present draft of the legislation. There are also many other, and more complex, examples.

The bill also appears to cover, and preclude, certain necessary business relationships. GCI offers a filtering service for subscribers who wish to preclude access to certain websites; GCI obtains the filtering service by outsourcing to another vendor. GCI must provide that vendor with certain subscriber information, and that vendor can also collect subscriber information. Similarly, GCI provides "wholesale" Internet service to other retail ISPs, such as Chugach Electric Association. GCI and Chugach must share subscriber information simply to establish service and bill the account. The bill would even appear to forbid GCI from allowing customers to pay their bill by a credit card, because GCI would then have to disclose the credit card number to the bank, or from referring a delinquent account to a collection agency.

There is also a significant question of whether it is practical (or even legal) for the State of Alaska to regulate this important element of interstate commerce. Several national ISPs, such as AOL, provide service to subscribers in Alaska. We believe that it is highly unlikely that large, nationwide providers will be able to modify services for Alaska subscribers to conform, for example, with the notification requirements of the bill; such providers will likely argue that complying with different requirements in 50 different states is an impossible burden unlawfully interfering with interstate commerce. The result could be that in-state providers are burdened with requirements that do not apply to national providers.

Finally, the definition of "subscriber information" remains too broad. For the same reasons that "electronic mail address" was deleted from the list of subscriber information, the subscribers' address and telephone number should also be deleted.

For all of the foregoing reasons, GCI cannot support HB 273 at this time. We would be happy to work with you and your staff to try to resolve these issues.

Sincerely,

David J. Porte
Vice President & General Manager
Internet Services

cc: Carolyn Johnson, Chugach Electric
Reed Stoops
Internet Alaska

Alaska Civil Liberties Union
P.O. Box 201844
Anchorage, AK 99520-1844
phone (907) 258-0044
fax (907) 258-0288
e-mail: akclu@alaska.net

March 24, 1999

Testimony to the House Labor and Commerce Committee

Regarding House Bill 273 relating to disclosure of personal information by an internet service provider.

House Bill 273,.

Comments of the Alaska Civil Liberties Union

The Alaska Civil Liberties Union wishes to thank Representative Kerttula for introducing House Bill 273, addressing the important issue of internet privacy, and thank the House Labor and Commerce Committee's hearing this bill.

This measure gives important statutory support to the goal of protecting individual rights and personal dignity in the new era of electronic communication.

The Alaska Civil Liberties Union supports the language of HB273, requiring that affirmative consent be obtained from a subscriber prior to the release of any personal information by an internet service provider about that subscriber.

The Alaska Constitution is clear about the right to privacy, and in the face of technological change this legislation is an important and necessary.

Requiring that an internet service provider obtain consent before disclosing personal information about a subscriber is a most basic provision in a computer-based environment where every purchase, any expression of interest or curiosity, all messages in or messages out can be tracked and monitored.

We urge the Committee to consider this bill and move its provisions forward.

(7) HOUSE COMMITTEE REPORT

Date Referred to Committee: January 10, 2000 FURTHER REFERRALS: Judiciary

Date of Committee Action: 24 MAR 2000

The LABOR AND COMMERCE Committee considered: HB 273

HOUSE BILL NO. 273 INTERNET SERVICE PROVIDERS

"An Act relating to the disclosure of subscriber information by Internet service providers."

recommends it be replaced with the following committee substitute CSHB 273(L+C)

[✓] the same title
[ ] a new title

[ ] additional referral to _____ _____ Committee
[ ] attached amendment(s)

ADOPTS: _____ Letter of Intent

ATTACHES NEW FISCAL NOTE(s): (Dept)

[ ] fiscal note(s) _____

[✓] zero fiscal note(s) LAW 3/17/00

APPROVES PREVIOUS: (Dept/Date)

[ ] fiscal note(s) _____

[ ] zero fiscal note(s) _____

| SIGNING WITH RECOMMENDATIONS | DP | DNP | NR | AM |
|---|---|---|---|---|
| | ✓ | | | |
| | | | ✓ | |
| | ✓ | | | |
| | | | ✓ | |
| | | | ✓ | |
| | | | ✓ | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

CHAIR'S SIGNATURE _____ 3-24-2000

# BusinessWeek

MARCH 20, 2000

A PUBLICATION OF THE McGRAW-HILL COMPANIES


## The Stock Market
Bargains in the Old Economy

## Warren Buffett

Why he's in a slump

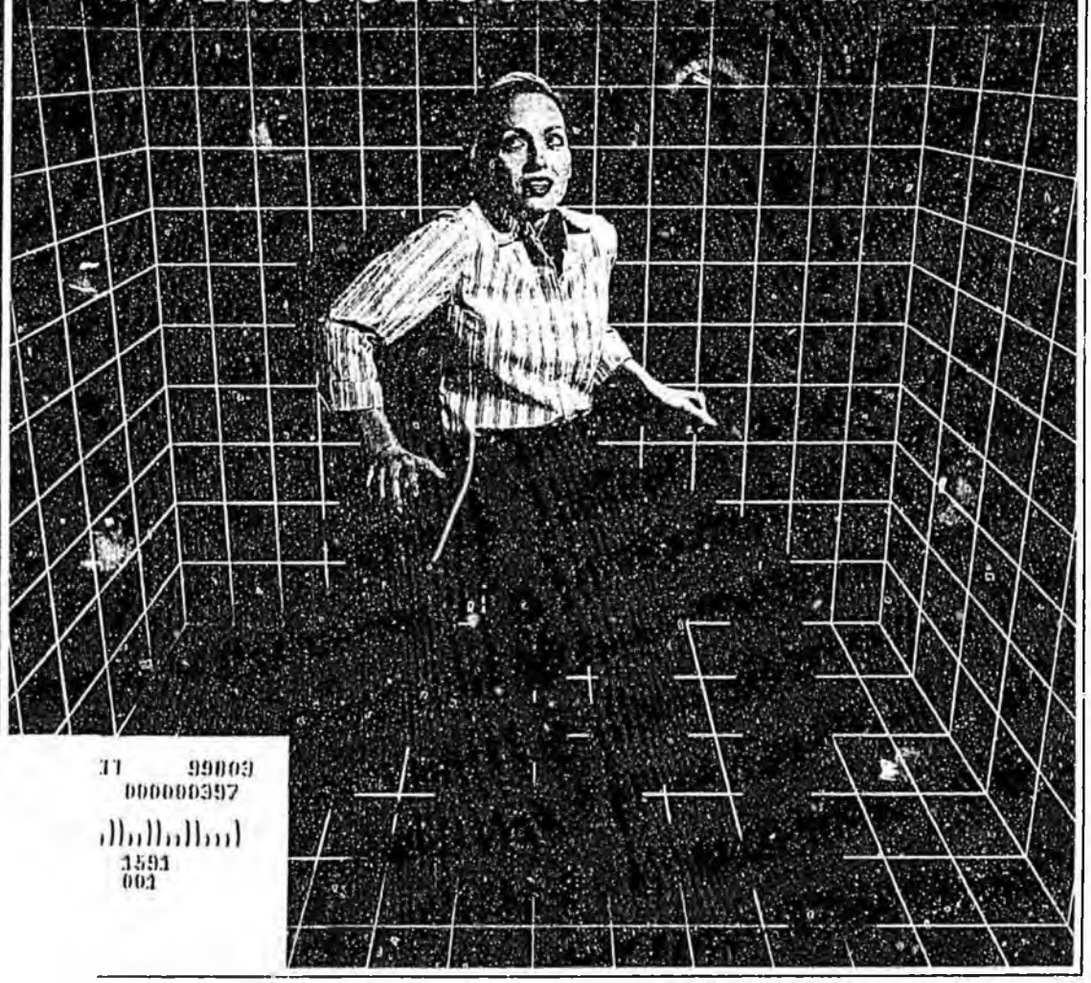
## The Disabled

Enlisting a new workforce

## Web Auctions
Curse of the winner


# PRIVACY ON THE NET

## What Should Be Done
PAGE 82





www.businessweek.com AOL Keyword: BW

ONLINE PRIVACY

# IT'S TIME *for* RULES *in* WONDERLAND

**Cover Story**

## Here's BUSINESS WEEK's four-point plan to solve the Internet privacy mess

IF LEWIS CARROLL HAD WRITTEN ABOUT ALICE'S ADVENTURES today, she would find herself passing through the looking glass and into cyberspace. She would meet up with dodos, duchesses, and eggheads, some of whom would spout the rough equivalent of "'Twas brillig, and the slithy toves...." The journey also would be full of rude surprises. As in Carroll's books, she would eventually discover who she really was. But many others she had never met would learn about her, too. Indeed, with every click of the mouse, a bit more of her privacy would vanish down the rabbit hole.

These days, a lot of people are stumbling on similar unpleasant surprises. Thanks to a string of privacy

ILLUSTRATION BY KATHY WEN

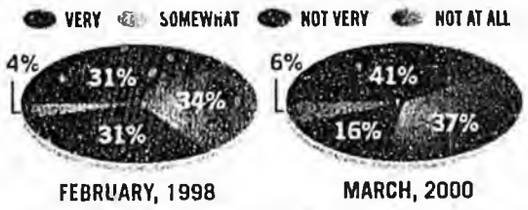
gaffes involving DoubleClick, RealNetworks, Amazon.com, and other major Web sites, consumers are learning that e-commerce companies have an intense interest in their private information. For about 9¢, some medical data sites will sell you your neighbor's history of urinary tract infections. Your speeding tickets, bounced checks, and delayed child-support payments are an open book. In the background, advertising services are building profiles of where people browse, what they buy, how they think, and who they are. Hundreds of sites already are stockpiling this type of information—some to use in targeted advertising, others to sell or trade with other sites.

**GOLD RUSH.** It will get worse. The tricks being played today are child's play compared with what's coming. Web sites that want to know you better will soon be able to track your movements on Web phones, palm devices, and video games, and parse the data with more subtle software. Online services can be layered with mounds of data about each person. Interactive TVs, for instance, have the potential to correlate the Web sites you visit at work with the ads you see at home in the evening.

Web surfers don't need extra proof that this gold rush for personal data is alarming. In a new BUSINESS WEEK/Harris Poll (page 96), 92% of Net users expressed discomfort about Web sites sharing personal information with other sites. The public outcry has grown so loud that in February, search engine AltaVista Co. promised to ask explicit permission before sharing visitors' personal information with other companies. On Mar. 2, DoubleClick bowed to public pressure on a similar point: The company, which serves up ads on many Web sites, has created anonymous digital snapshots, or "profiles," of millions of cybersurfers, based on where they browse and what they do online. DoubleClick had planned to link profiles with much more specific information, including names and addresses culled from real-world databases that cover 90% of American households. The company dropped that controversial plan, and within days, smaller rival 24/7 Media Inc. abandoned a similar strategy.

## A RISING TIDE OF CONCERN...

If you shop online, how concerned are you that the company will use your personal information to send you unwanted information?



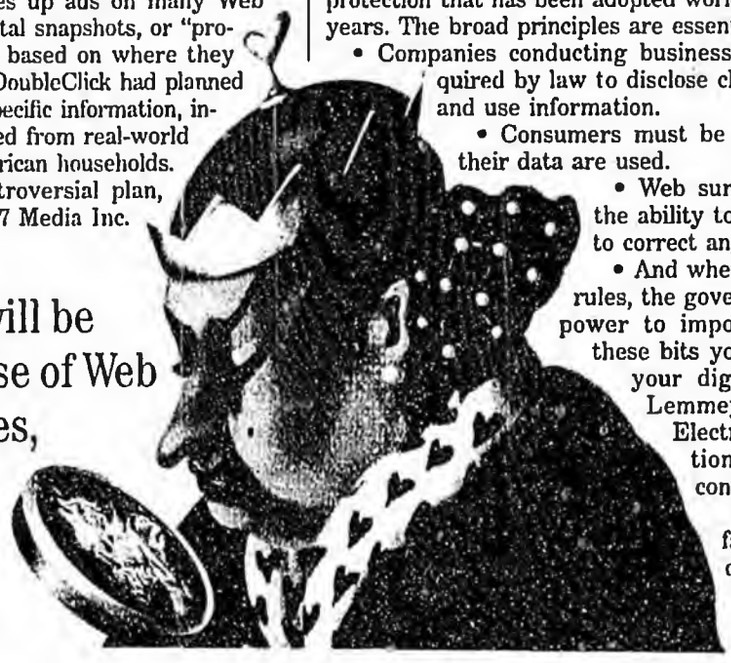

If you don't buy online, how concerned would you be that, if you did, a company would use personal information to send unwanted information?


## ...COULD BE ALLAYED BY GUARANTEES

If you use the Internet, to what extent would explicit guarantees of the security of personal information encourage you to buy online?


NOTE: "DON'T KNOW" AND "REFUSED" NOT INCLUDED. FULL RESULTS, PAGE 96
DATA: BUSINESS WEEK/HARRIS INTERACTIVE POLL OF 1,014 PEOPLE

Soon cybersnoops will be able to track your use of Web phones, palm devices, and video games



Anonymous tracking and profiling by DoubleClick and 24/7 can be very subtle. But sometimes privacy violations hit you in the face. We have all heard the examples of sociopaths who stalk their victims online. We have seen the statistics on "identity theft," in which criminals suck enough personal data off the Net to impersonate other people. Perhaps these are extreme examples. Even without them, many cybersurfers are starting to feel that they have spent quite enough time at this particular Mad Tea Party. They are ready for privacy rules that set some plain and simple boundaries. In the March BUSINESS WEEK/Harris Poll, 57% of respondents said government should pass laws on how personal information is collected. "What's going on today is exponentially more threatening to those who want to protect privacy," says Eliot Spitzer, New York's state attorney general who has proposed privacy legislation. People can't make informed decisions on the Net because they lack the necessary information. "What we're confronting is a market failure," says Spitzer.

Responding to a growing chorus of privacy-related complaints, some states have drafted legislation ranging from curtailing the sale of personal information to the creation of a privacy ombudsman. But this piecemeal, state-by-state approach is a muddle. Scattershot laws will only create more confusion. Over time, they will choke budding e-business in complex litigation and red tape.

BUSINESS WEEK believes there is a better way. Instead of a conflicting patchwork of state rules, the federal government should adopt clear privacy standards in the spirit of the Fair Information Practices—a philosophical framework for privacy protection that has been adopted worldwide over the past 25 years. The broad principles are essential:

- Companies conducting business online should be required by law to disclose clearly how they collect and use information.
- Consumers must be given control of how their data are used.
- Web surfers should also have the ability to inspect that data and to correct any errors they discover.
- And when companies break the rules, the government must have the power to impose penalties. "All of these bits you are sending out are your digital DNA," says Tara Lemmey, president of the Electronic Frontier Foundation. "You should have control of that."

Regulation flies in the face of the approach industry has been chum-

pioning. For the past four years, Net companies have insisted that they can police themselves on privacy. "Industry initiatives and market forces are already doing a good job," says Daniel J. Jaye, co-founder of Engage Technologies Inc., which dishes up ads on the Web.

In other words, the market will punish companies that fall afoul of consumers. Bringing in the government, execs say, will pile bureaucratic layers on top of the Net. This could undercut the very promise of efficiency that many online businesses are counting on. The Internet, they say, is supposed to draw companies closer to their customers, allowing them to anticipate their desires. With profile data, they can target their ads, slash wasteful and random marketing costs, design products faster, and build higher profit margins. Profiling provides the underpinnings of a new way of doing business upon which the Net Economy is built.

Laws that require businesses to seek users' permission before they collect or use data about Web-surfing habits could kill this goose, they say. And why do that, industry execs ask, when they are making such fine strides in protecting consumer privacy? As a positive sign, Net businesses trumpet a May, 1999, Federal Trade Commission survey in which 66% of companies queried had privacy policies.

**SELF-REGULATORY SHAM.** We are not persuaded by these arguments. Few Web sites give consumers real choices over the data that get collected online. There is no proof that if given a choice—especially bolstered with financial incentives proffered by Web merchants—consumers won't willingly hand over some personal data. As for privacy policies, the same FTC survey showed that while more than 90% of companies polled collected personal information, fewer than 10% actually followed all of the established Fair Information Practices.

In short, self-regulation is a sham. The policies that companies have posted under pressure from the government are as vague and confusing as anything Lewis Carroll could have dreamed up. One simple example: When people register at Yahoo! Inc. for one of its services, such as My Yahoo, they are asked to provide their birth date and e-mail address—ostensibly as a safeguard if they forget their user name and need prompting. But Yahoo also uses that information for a service called the Birthday Club, sending product offers from three to five merchants to users via e-mail on their birthday.

> Because privacy breaches are so corrosive to consumer trust, some Web executives welcome broad national standards

Don't look for transparency here. Most sites don't limit how they or their partners use consumer information. And Web sites can transfer information to partners without telling their own customers. Many sites also change their practices at will and without warning.

Because privacy breaches are so corrosive to consumer trust, some Web execs actually welcome broad national standards. IBM and Walt Disney Co. have decided not to advertise on Web sites that don't have privacy policies. Privacy codes must be clearer, says Chris Larsen, CEO and founder of E-Loan Inc., an online loan service that has its privacy policies audited. "I think the industry has squandered the opportunity to take care of this on its own." IBM Chairman Louis Gerstner doesn't go that far. But he has warned Net executives that they must get serious. "I am troubled, very troubled, by leaders who have failed to recognize our responsibility in the transformation of the new economy," he says.

We hope other Web execs are listening closely. The policies we propose are in the best interests of Web businesses. If more consumers can be assured that their personal informa-

## ❖ THE LANGUAGE *of* ONLINE PRIVACY ❖

**COOKIES** These tiny software programs keep a log of where people click, allowing sites to track customers' habits. Cookies are placed on consumers' computers when they first visit sites or use things like online calendars, personalized news services, or shopping carts.

**ONLINE PROFILING** By using cookies, sometimes combined with personal information, sites build profiles about what customers do or don't buy, what they look at, how much time they spend in different areas, and what ads they click on.

**REFERERS** Information that your Web browser passes along when you move from one site to another or use a search engine or even just send an e-mail. Referers can be collected and used to target advertising.

**ADVERTISING NETWORKS** The Net equivalent of ad agencies, the most famous being DoubleClick, Engage, and 24/7. They amass millions of profiles of Web surfers based on their online habits. Ads are then aimed at those most likely to buy what is being pitched.

**REGISTRATIONS** Anywhere you fill out personal information in order to download software, sign up for a free service, or buy something online. The data can be sold or shared with other Web sites or advertisers.

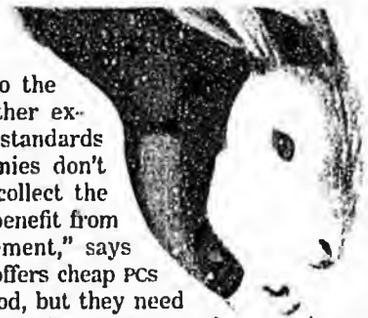
**IP ADDRESS** A number automatically assigned to your computer whenever you connect to the Net. The numbers are used by network computers to identify your PC so that data can be sent to you. But addresses can be used in profiling and ad targeting.

**PRIVACY POLICIES** Notices posted on a Web site that disclose how a company collects, uses, and shares data with partners or advertisers. These sometimes include opt-in and opt-out buttons.

**OPT-IN AND OPT-OUT** Privacy choices that some Web sites offer to their visitors. In opt-out situations, the site is free to gather and sell information on you unless you specifically tell it not to by clicking on a button. With opt-in, gathering or selling your data is forbidden unless you click to give permission.

**PERSONALLY IDENTIFIABLE INFORMATION** Your name, address, or credit card number and other details linked to your real-world identity.

**THIRD-PARTY DATABASES** Companies like Acxiom and Experian stockpile information such as name, address, phone number, and income on most U.S. households. Increasingly, these companies are working with Web sites and software makers.



Some 20 states are moving to protect Net privacy. A federal effort would cut costs and complexity

tion is safe, more of them will flock to the Net—and click, not exit. There are other explicit benefits for the industry. Privacy standards create a level playing field, so companies don't fall into an arms war, each trying to collect the most data—at any cost. "Business will benefit from the right level of government involvement," says Nick Grouf, founder of PeoplePC, which offers cheap PCs and Net connections. "Standards are good, but they need some teeth, and this is where government becomes a good partner."

**FEDERAL STANDARD.** In the long term, the privacy protection that BUSINESS WEEK espouses will make life simpler for businesses on the Net. More than 20 states already are moving to enact some kind of guarantees. A minimum federal standard of online privacy would decrease the cost and complexity for companies. It also would increase trust. If businesses really want to be close to their customers, trust is paramount. This approach also will shrink the gap that has arisen between the U.S. and Europe, where privacy already is recognized as a right. The Europeans have stood firm, putting American companies in the peculiar position of extending greater privacy protection in Germany or France than at home.

It's time to iron out the inconsistencies. Here are our prescriptions for protecting personal privacy without jeopardizing the promise of e-commerce:

****************

# OUR FOUR-POINT PLAN

## E-privacy and e-commerce can coexist. Here's how to safeguard both

### ❶ DISPLAY YOUR PRACTICES

Privacy policies seem like very simple things. Companies put up a notice online about how they gather and use information, and it's win-win from there. Consumers get the lay of the land, and Net companies pass on to consumers the responsibility for their online privacy.

If only it were that simple. These little postings have actually been the focus of rancorous debates for years. The tricky thing is that once policies are up there for all to see, companies are legally obligated to uphold them. That's one reason sites have dragged their feet in putting them up. Or should we say down? The statements are usually buried at the bottom of the page, and seem to be drafted by life-forms on a distant planet.

It's time that policies be written for mere mortals. Not many sites do a great job of explaining how information is tracked, used, and disclosed to partners. Consider the privacy policy of search engine Ask Jeeves. The company first says it always asks permission before providing information to partners. Yet on a registration form, the choice given to consumers is that information is shared unless you say otherwise. To confuse matters further, the policy later states that: "Ask Jeeves sometimes co-sponsors [sweepstakes and contests] with other companies, in which case the user's individual contact and demographic information is likely to be shared with participating sponsors. [The] information will not be released... without the user's consent." So which is it: Is your information automatically shared unless you go the extra step to object? Or is it kept private unless you pipe up and give the green light? When asked directly, Ask Jeeves says it depends. Depends on what? It's fine for companies to have different options, but too vague possibilities baffle consumers, rendering privacy notices useless.

One solution might be simple icons that help to navigate the policies. Like the "Information" sign that is recognized around the world, these symbols could be standardized: a large "p" signifying "privacy policy" could be placed on the top right-hand side of the page, on a registration form, in an electronic shopping cart, or anywhere that information is collected on a site. Often it's not clear, upon registration, whether you need to locate an "opt-out" button and click on it to stop the site from sharing your information with others, or whether the site intends to ask your permission each time it wants to pass information to another site. Icons could help clarify this (page 88).

**SECOND OPINION.** Simple road signs on the Info Highway may seem trivial, but understanding the full measure of privacy policies is no joke. They resemble contracts. Indeed, they are generally the only privacy-related feature on sites that can actually trip a lawsuit. In January, New York District Attorney Spitzer used privacy policy violations by Chase Manhattan Bank and Sony Music Entertainment Inc.'s InfoBeat to curtail their sharing of data. "We have an obligation to define reasonable boundaries," he says. "We have to articulate what privacy rules should be and then how to enforce them."

It isn't enough to have just any old policy, though. The statements need to follow the Fair Information Practices, clearly laying out how each site addresses choice, access, and security. Policies should outline how a person's information is shared and how to limit its use. Contact numbers or e-mail addresses should be available. And the date on when the policy was last changed should be clearly stated. Web execs make a good argument when they say that it's hard to know how they will use data in the future. But they should alert consumers when the policy changes. Amazon.com, for example, says it doesn't sell or trade information now, but adds: "We may choose to do so in the future." The only notice the company says it will give is a change in its policy online.

The sharing of information is a white-hot button in the privacy debates. And for good reason. A Georgetown University survey of the privacy policies on health-care sites showed how common this is. Of 21 sites sampled, six offered assessments on health conditions that were actually run by other companies. Some companies shared names, ages, and e-mail addresses, which makes it hard for users to know who

has their personal data or which privacy policy to rely on.

In the best of all worlds, companies should bind partners with whom they share data to their privacy policies. At the very least, they should inform consumers that they plan to transfer personal information to a partner. That way, consumers can check out the partner's privacy policy and make an informed decision about whether they want to participate.


**DEFINING TERMS.** It's all too vague on Yahoo's Web site. That's partly because the No. 1 site on the Net has what's known as a "universal registration," where people sign up once and are entitled to a host of different services—from e-mail to auctions to private personal calendars. But the universal registration information also ties in with other services offered through partners, such as the reservation service Travelocity provides. While details about data-sharing practices are explained on Yahoo, they are buried many clicks deep in so-called terms of service agreements, which aren't marked as privacy policies.

Some companies, such as PeoplePC and eBay, have very clear policies that give descriptions of how information could be passed to partners and naming some partners as examples. They also try to provide some level of surety. For instance, eBay Inc. says that before it provides personal information to partners, it lets users see the data it has collected. That's a step forward, but still limiting. To prevent eBay from sharing your data, you must choose not to use the service. And for those who give the O.K.? Once the information is transferred in these co-branded services, eBay says it has no control over how partners use the data.

It's crucial that these partnerships, data-gathering techniques, and customer options are spelled out, especially for Net newbies. Companies must be clear about how they define "personally identifiable information," because that description can change from site to site. Just as vital, they need to spell out the technology used to track and profile consumers. RealNetworks, which overhauled its privacy policies this fall after being accused of compiling information about the musical tastes of users, has a straightforward approach. It breaks out every tracking technique it uses and explains them simply and effectively. In contrast, CBS SportsLine explains that it uses IP addresses to identify users and their shopping carts but doesn't bother to explain what an IP address is. For the record: This is a trackable number assigned to your PC every time you connect to the Web.

> DISCLOSURE
> "This doesn't make any sense," she said. "You are obliged under law to spell this out more clearly"

Clearly, privacy policies are backbreakers to write. But it seems the hardest part about them for any company is coming up with a privacy philosophy that they will stick to. Once this hurdle is crossed, however, the positive impact might resonate into the brick-and-mortar world as well. Privacy policies governing credit reports, drug prescriptions, and more could follow the new model for the Internet.

## ❖ HOW TO DRAW *the* LINE ❖

**DISPLAY YOUR PRACTICES** Privacy policies should be mandatory, easy to find, and written in plain English. Companies should clearly state why they are collecting information and collect no more data than they need for that purpose. Data collected for one purpose shouldn't be used for another without consent. A simple set of icons should be developed to warn people about privacy threats.

**GIVE PEOPLE A CHOICE** If a business wants to collect information about a consumer's health, finances, or sexual orientation, it should ask them for permission first. This allows a Web surfer to opt-in. The same rule applies if the company wants to resell personal data or share it with advertising networks. In all other situations, users should be given the option to withhold their information by checking a prominently displayed, easy-to-understand box. This is called opt-out.

**SHOW ME THE DATA** Consumers must have the ability to look at and correct sensitive information, such as financial and medical data. There should also be a mechanism for double-checking a profile that combines personal information with online habits or is shared with another company. This is especially urgent when a profile triggers offensive or unwanted marketing solicitations. Web sites and marketers should share the responsibility for this.

**PLAY FAIR OR PAY** These rules won't enforce themselves. A broad law ensuring privacy online must be passed at a federal level. An agency, such as the FTC, would enforce and interpret the law according to the Fair Information Practices. Companies should also periodically disclose their practices in some kind of public record, such as SEC filings or trusted third-party audits.

## DANGER! DANGER!

*Nothing gets people's attention like a good, loud warning sign. For those who don't have the patience to burrow through privacy policies, here's a set of icons that could flag potential perils.*

This site collects financial information

This site collects health information

This site transfers data to other companies

Privacy policy located here

Opt-In

Opt-Out

# ❷ GIVE PEOPLE A CHOICE

Right now, there's only one way you can be sure that the sensitive details of your life won't spill out over the Internet: Don't log on in the first place.

Short of doing that, consumers who surf the Web do so at their own peril. There are practically no laws to stop sites from ferreting out as much personal information about you as they can get their hands on—and then turning around and selling it to the highest bidder. If an AIDS patient visits a health site to investigate the side effects of the drug AZT, that site is free to market the information to drug companies, insurers, or anyone else.

Things don't have to be this open. What is needed is a way to give consumers more control over what is collected about them and more say over how it can be used. Proposed new federal and state laws would require Web sites to allow consumers to "opt out" of a company's data-collecting and resale operations. How? The new laws would force sites to display a box, which, for example, could be checked off by AIDS patients if they didn't want health-care sites to track the screens they read, store their credit card numbers, or resell any of that information.

**OPTING OPTIONS.** Of course, many Web sites already let visitors opt out. But most of those opt-out boxes are buried. Some of the proposed new privacy laws, such as a Senate bill being sponsored by Ron Wyden (D-Ore.) and Conrad Burns (R-Mont.), would require every Web site to offer a clearly written, prominently displayed opt-out box. Under such bills, consumers who arrive at the home page of Yahoo, Amazon, or eToys, would be able to find the opt-out box right under their nose, perhaps on the upper righthand corner of their screen.

But even such prominently placed boxes might not be protection enough. Studies indicate that people who may otherwise be worried about online privacy are not going to stop their surfing long enough to read a few sentences of dense boilerplate, and then click on a box. That's why some politicians and privacy advocates are pushing even tougher protections. Rather than put the burden on consumers to opt out, they want to put the burden on companies to get Web surfers to opt in. Before a site could start collecting and selling most data, it would have to get people to check a box giving it permission to do so. A controversial Senate bill to do this has been proposed by Robert Torricelli (D-N.J.).

Industry reaction to giving consumers more choice ranges from genuine enthusiasm to hyperventilating hostility. Among critics, opt-out legislation is generally regarded as the lesser evil. But because information technology is evolving rapidly and the Internet soon will be widely available on tiny cell phones and other devices, some online executives worry that a bulky, federally required opt-out notice might not fit. "Having laws get down to pixel counts and screen layouts won't work," says Max Metral, chief technology officer for PeoplePC.

Nonetheless, most Web executives can live with opt-out. But they are terrified of opt-in. Execs worry that many people simply won't be willing to make the extra effort that opting in requires. As proof, some cite the Children's Online Privacy Protection Act, a 1998 law that limits the collection of information about kids under 13. Among other things, COPPA requires parents to opt in, by written letter or fax to the site, before their children can use online chat rooms and message boards. Just ask Julie Richer, president of San Francisco-based cyberkids.com, a site that targets 7- to 12-year-olds. Richer says COPPA has caused message board and chat room traffic to plummet by more than 40%.

But the objections to the opt-in rule go beyond the issue of reduced traffic. Advertising revenues might also suffer under Torricelli's opt-in proposal. There would be less free information available, making it harder for companies to put together the kinds of demographic profiles that allow them to target customers more precisely. Says DoubleClick President Kevin Ryan: "The Torricelli legislation would have a very negative impact on the Internet."

There's no doubt that opt-in would hike the cost of doing

## INFORMED DECISION

"Do you wish to reveal personal medical information at this site?" he asked. "If so, this is how we'll share the data with others"

business online. But it's not as bad as its detractors claim. For one thing, companies would be able to lure people to opt-in by offering Web surfers cash and other incentives. It also would earn the goodwill of privacy-conscious Web surfers. One convert is Gregory Miller, chief Internet strategist for MedicaLogic, a Hillsboro (Ore.) site offering online health information, and a member of the Federal Trade Commission's new advisory committee for online access and security. His company supports opt-in on the theory that customers will be attracted to a site that takes privacy concerns seriously. "If you ask someone for permission to market to them, you build a loyal customer," says Miller. "It's our job to convince the consumer that it's a good idea to opt in by being truthful and showing what the benefit is." One way MedicaLogic would do this: It could persuade diabetes sufferers to surrender their personal information by offering timely updates on advances in treatment. "There are so many users out there, and the Net is growing so rapidly, that you can still get a reasonable return on your investment. People can be persuaded to opt in," says Miller.

Ideally, the best way to protect privacy on the Net is to combine the best elements of both opt-out and opt-in—as the European Union does. Opt-in methods are relatively extreme, so they should be used only for the most sensitive information—your chronic heart problems, for example, or the details of your financial holdings and your sexual preferences. And rules should be strict. No pre-checking of the opt-in box allowed. Instead, companies should be forced to describe what type of information they will be collecting and what they will be doing with it. Finally, opt-in also should be required before a company can resell any information about a Web surfer to a third party or share it with an ad network, since this offers few benefits to the surfer.

Apart from these extreme situations, the rule should be opt-out. Yes, it will be a pain in the neck to offer consumers this much control over how their information is used. But the bigger hurt could come from doing nothing and watching Web surfers opt out of the Internet.

ACCESS

"I don't think you have understood me properly," she said. "Please show me the online profile that you have compiled about me"

## ❸ SHOW ME THE DATA

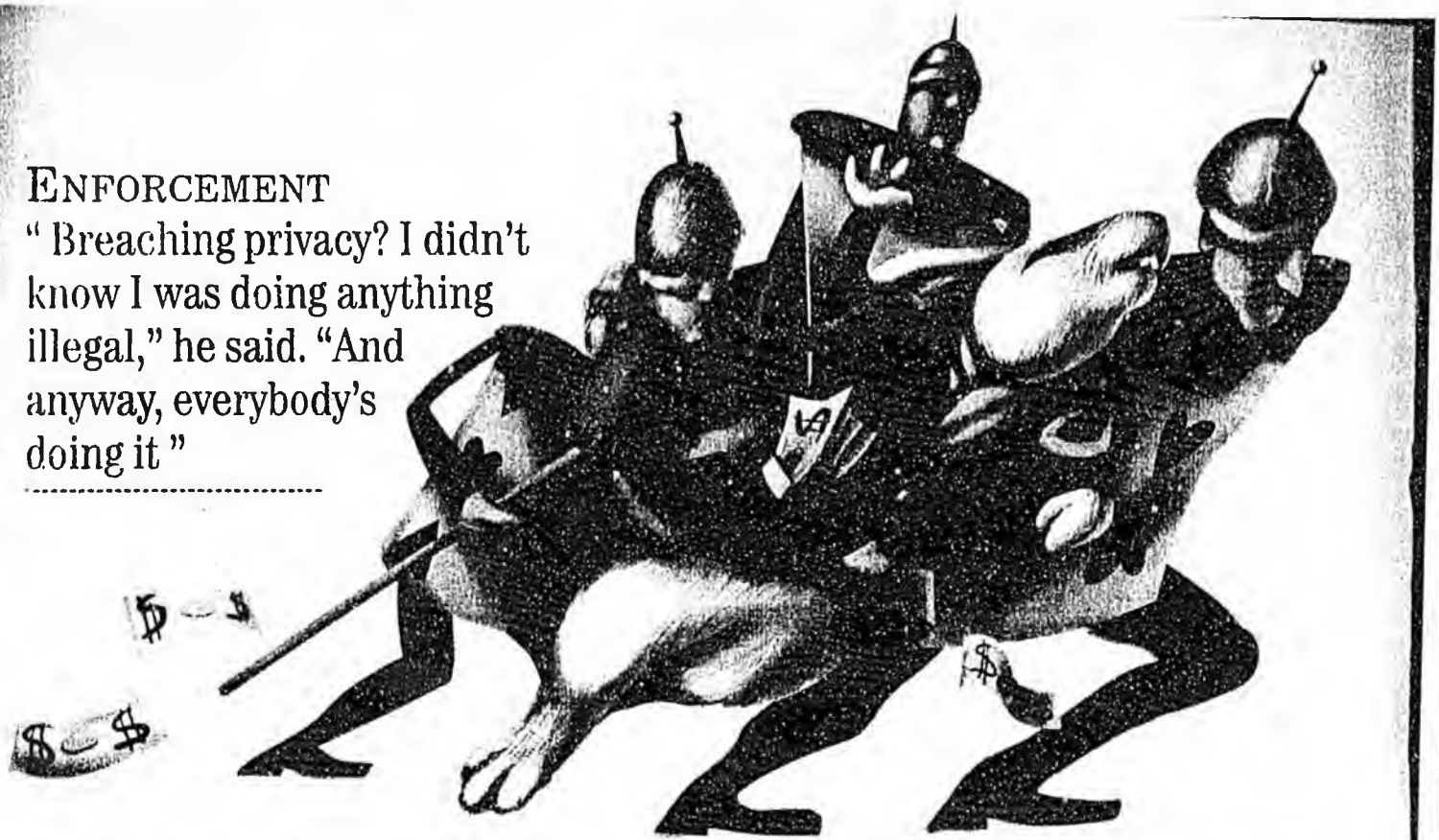
Americans gained a precious thing from the Fair Credit Reporting Act of 1970: the right to inspect their credit records and find out why the bank turned them down on a car loan or a mortgage. No such privileges exist when it comes to online profiles, and it won't be easy to invent them. But some experts say the same kinds of tools Web sites use to track visitors could be used to provide at least a partial window into the data banks that store online profiles.

First, the downsides of doing that: The information a Web site collects is often strewn among multiple databases. Companies may not have the resources to query each one every time a surfer gets curious. What's more, the profile of your browsing habits may be based on cookie files—the bits of identifying code that Web sites deposit on your hard drive so they can monitor your comings and goings. If that's the case, those profiles may be linked only to the computer you browse from, not to your identity in the outside world. Do you really want to request access to that profile? The site would have to authenticate you. And in the process, it would acquire even more information about you than it started with. "It's clear that many systems on the Web were designed without much thought to privacy," says David M. Kristol, a member of the technical staff at Lucent Technologies Inc.'s Bell Labs. "These systems may be quite difficult to retrofit."

Hard, but not impossible. Some of these challenges seem tailor-made for smart software solutions. "If there's data in a database, it's there so that you can access it," says Lorrie Cranor, an AT&T Labs researcher who chairs a privacy working group at the World Wide Web Consortium. Second point: If your profile—warts and all—is pegged to a string of numbers in cookie files, then, in theory, a Web site could manage your request for access by matching it to that same string. Authentication would be far from perfect, but perfection is rare in cyberspace. "We need a button we can push that says 'show me the profile you have on me,'" says personal privacy detective Richard Smith in Boston. "That should be relatively straightforward, because they already have an account mechanism, the sign-in." And if companies refuse? People could take it to the Fair Trade Commission.

The FTC, by the way, is on the case. It established an advisory committee on online access and security that began meeting on Feb. 4. It's made up of 40 people, including lawyers, professors, industry representatives and privacy advocates. And it plans to provide recommendations to the FTC on a range of options by May 15.

Not all the modes of online behavior that come before this committee will be so terribly controversial. Few argue against letting consumers see—and correct if neces-



ENFORCEMENT

" Breaching privacy? I didn't know I was doing anything illegal," he said. "And anyway, everybody's doing it "

sary—sensitive data such as financial records and medical data. But many execs say providing access to routine info would be a costly nuisance of dubious benefit to consumers. "Do you really need to see that Banana Republic says you bought five shirts when you bought four, and do you really need to correct that?" says a lobbyist for one Web company.

But even where it's a nuisance to business, consumers should see more of what goes on behind the curtain. If you're being hounded by a direct marketer who is convinced you are interested in sex toys, you should be able to see whose data generated this profile. The marketer will probably argue that the data are culled from too many places. But there's an easy answer to that, too: Make the marketers keep a source list. Computers excel at keeping track of such things. If they were bad at it, this privacy morass never would have happened.



## 4 PLAY FAIR OR PAY

Better warnings. More choice. Access to your personal records. These things will go a long way toward protecting your privacy. But they won't be enough. After passing the broad laws that we are proposing, Congress will have to take extra steps to insure that companies honor them.

The reason: Privacy laws are unusually hard to enforce. Say, for example, that you plug information about your stock portfolio into a financial Web site but deny permission for this information to be shared. Say that the site ignores your request and sells the data to a charity anyway. Most likely, you'll never find out about the privacy breach. And even if you do, the infraction didn't cause you any economic harm. That means you wouldn't have much financial incentive to sue the offender—and you'd no doubt have a hard time getting a lawyer to take your case. "Only people with a real privacy vendetta are going to sue," says Jonathan Zittrain, executive director of Harvard University's Berkman Center for the Internet & Society.

Because enforcement is chancy, unethical Web sites will be tempted to cheat on the rules. So, to ensure that crime does not pay, Congress will have to shell out a lot of money for privacy cops. Which agency should handle the job? Some experts have suggested creating a brand-new federal privacy commission—but that would be a political nightmare. Others have suggested a government-authorized, industry-run group such as the Internet Corporation for Assigned Names & Numbers (ICANN). This type of quasigovernmental organization would probably move faster than a typical agency, but it also would be vulnerable to becoming the pawn of the very people they're supposed to regulate.

We favor giving the job to the Federal Trade Commission, which has begun moving aggressively on the issue of Internet privacy and which already enforces the Children's Online Privacy Protection Act, the Truth in Lending Act, and the Fair Credit Reporting Act. The agency should be empowered to impose stiff penalties for violations.

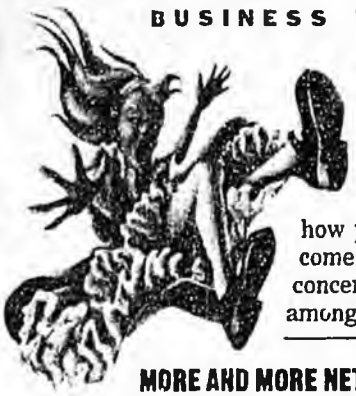
**PRIVATE PROTECTION.** Of course, any privacy laws will need to evolve. As the Internet makes its way onto cell phones, watches, and other devices, some of the privacy rules that make sense in a world of deskbound PCs may become irrelevant. And the long-term prospect of biometric authentication—where fingerprints and retinal scans may be used as New Age passwords to Web sites—will certainly raise serious new privacy issues. Such a scheme would require nothing less than a national database of identifying biological data, raising the spectre of abuse by both outlaw hackers and Big Brother prosecutors.

Meanwhile, new technologies will certainly emerge to help consumers safeguard their own privacy. This summer may see the launch of the long-awaited P3P software standard, which will provide the means for consumers to set privacy preferences in their browsers and allow them to be automatically alerted when the Web sites they click on have privacy policies that differ from their choices. But this technology won't be a panacea. Privacy isn't just about fancy software. It's also about making sure that information is being used in the ways companies had promised. Technology won't protect people from privacy invasions. Only people can do that.

*By Heather Green, Mike France, and Marcia Stepanek in New York, and Amy Borrus in Washington, D. C.*

The Cover package continues with a poll on page 96

BUSINESS WEEK/HARRIS POLL



# A GROWING THREAT

Cover Story

Concern is rising over privacy on the Net, with a clear majority—57%—now favoring some sort of laws regulating how personal information is collected and used. Regulation may become essential to continued growth in e-commerce, since 41% of online shoppers say they are very concerned over the use of personal information, up from 31% two years ago. Perhaps more telling, among people who go online but have not shopped there, 63% are very concerned.

## MORE AND MORE NET SHOPPERS

If you go online from home, work, or another location, have you ever used the Internet, World Wide Web, or online service to purchase anything?

| | MARCH, 2000 | FEBRUARY, 1999 | FEBRUARY, 1998 | SEPTEMBER, 1997 |
|---|---|---|---|---|
| Have purchased | 45% | 31% | 23% | 19% |
| Have not purchased | 55% | 69% | 77% | 81% |

## ONLINE BUYERS DREAD J'UNK MAIL

If you have made online purchases, how concerned are you about each of these possibilities?

| | VERY CONCERNED | SOMEWHAT | NOT VERY | NOT AT ALL |
|---|---|---|---|---|
| The company you buy from uses personal information you provide to send you unwanted information | | | | |
| March, 2000 | 41% | 37% | 16% | 6% |
| February, 1998 | 31% | 34% | 31% | 4% |
| The company or one of its employees uses your credit-card information to make purchases without your consent | | | | |
| March, 2000 | 39% | 31% | 22% | 7% |
| February, 1998 | 56% | 25% | 12% | 7% |
| In the course of the transaction, your credit-card information is made accessible to others who might use it without consent | | | | |
| March, 2000 | 42% | 34% | 17% | 6% |
| February, 1998 | 56% | 28% | 11% | 3% |

## NONBUYERS WORRY ABOUT PRIVACY AND FRAUD

If you go online but have not purchased anything, how concerned would you be about each of these possibilities if you were to buy anything?

| | VERY CONCERNED | SOMEWHAT | NOT VERY | NOT AT ALL |
|---|---|---|---|---|
| The company you buy from uses personal information you provide to send you unwanted information | | | | |
| March, 2000 | 63% | 31% | 4% | 2% |
| February, 1998 | 52% | 34% | 11% | 3% |
| The company or one of its employees uses your credit-card information to make purchases without your consent | | | | |
| March, 2000 | 71% | 18% | 7% | 4% |
| February, 1998 | 80% | 12% | 6% | 2% |
| In the course of the transaction, your credit-card information is made accessible to others who might use it without consent | | | | |
| March, 2000 | 76% | 20% | 3% | * |
| February, 1998 | 86% | 10% | 2% | 1% |

## AN ONLINE PROFILE IS DISCOMFORTING

Some Web sites track users' personal information to match users with products and services that meet the users' needs. Other Web sites profit by sharing or selling user information to other organizations. If you use the Internet, how comfortable would you be if a Web site did the following?

| | VERY COMFORTABLE | SOMEWHAT COMFORTABLE | NOT VERY COMFORTABLE | NOT AT ALL COMFORTABLE | DON'T KNOW |
|---|---|---|---|---|---|
| Tracked your movements when you browsed the site, but didn't tie that information to your name or real-world identity | 9% | 28% | 28% | 35% | * |
| Merged your browsing habits and shopping patterns into a profile that was linked to your real name and identity | 3% | 7% | 21% | 68% | 1% |
| Created a profile of you that included your real name and identity as well as additional personal information such as your income, driver's license, credit data, and medical status | 3% | 2% | 13% | 82% | 0% |

## A PRIVACY GUARANTEE WOULD HELP

If you go online, to what extent would a policy that explicitly guarantees the security of your personal information encourage you to do the following?

| | A LOT | A LITTLE | NOT AT ALL | DON'T KNOW |
|---|---|---|---|---|
| Use the Internet more in general | | | | |
| March, 2000 | 40% | 40% | 19% | 1% |
| February, 1998 | 18% | 44% | 38% | * |
| Register on that Web site, providing personal information | | | | |
| March, 2000 | 30% | 39% | 31% | 1% |
| February, 1998 | 12% | 44% | 44% | * |
| Purchase products or service from that company | | | | |
| March, 2000 | 37% | 36% | 26% | 1% |
| February, 1998 | 15% | 42% | 43% | 0% |

If privacy notices let you "opt out"—in other words, you could choose not to have your personal information collected by a particular Web site—how often would you "opt out?"

| | |
|---|---|
| Always | 56% |
| Sometimes | 34% |
| Rarely | 4% |
| Never | 6% |

## A MAJORITY OF ALL PEOPLE POLLED FAVOR NEW LAWS

Here are three ways tha he government could approach Internet privacy issues. Which one of these three do you think would be best at this stage of Internet development?

| | MARCH, 2000 | FEBRUARY, 1998 |
|---|---|---|
| The government should let groups develop voluntary privacy standards, but not take action now unless real problems arise | 15% | 19% |
| The government should recommend privacy standards for the Internet, but not pass laws at this time | 21% | 23% |
| The government should pass laws now for how personal information can be collected and used on the Internet | 57% | 53% |
| None of the above | 1% | 2% |
| More than one of the above | * | 0% |
| Don't know | 5% | 3% |
| Refused | 1% | * |

Telephone survey of 1,014 adults between Mar. 2 and Mar. 6 by Harris Interactive. Except where noted, don't know and refused not included. Some categories do not total 100% due to rounding.

*Less than 0.5%

BusinessWeek ONLINE For more complete results and related stories, see the Mar. 20 issue of www.businessweek.com.