

Privacy -- On-Line

A Selection of Current Law, Cases, and Legislation of California ♦ United States ♦ International

Prepared By: *Lynn M. Holmes, Esquire*
Attorney & Counselor-At-Law
PO Box 207, Forestville, CA 95436
Phone 707-887-9399
E-mail: lynn.holmes@usa.net

Last Updated: December 7, 2000
Revision 3

Copyright 2000 Lynn M. Holmes. All rights reserved.

Points of view or opinions expressed in these pages are those of the author. Nothing contained herein is intended to address any specific legal inquiry, nor is it a substitute for independent legal research to original sources or obtaining separate legal advice regarding specific legal situations.

To obtain additional copies please contact the author:
Lynn M. Holmes, Esquire – PO Box 207, Forestville, CA 95436,
Phone: 707-887-9399, Fax: 707-887-8387 E-Mail: lynn.holmes@usa.net

Table of Contents

I. ON LINE PRIVACY	1
A. PERSONAL INFORMATION OR PERSONAL IDENTIFYING INFORMATION – WHAT IS PRIVATE INFORMATION? 2	
II. CALIFORNIA – EXISTING LAW	3
A. CALIFORNIA CONSTITUTION – INALIENABLE RIGHTS: PRIVACY	3
B. INFORMATION PRACTICES ACT OF 1977	4
1. <i>Customer Records: Personal Information: Disposal</i>	4
C. CALIFORNIA PUBLIC RECORDS ACT.	5
D. PERSONAL INFORMATION: COLLECTION AND DISCLOSURE – THE OFFICE OF PRIVACY PROTECTION.....	5
E. CONSUMER CREDIT REPORTING: MEDICAL INFORMATION.....	6
F. AREIAS CREDIT CARD FULL DISCLOSURE ACT OF 1986: CREDIT CARDS; MARKETING INFORMATION ...	6
G. SUPERMARKET CLUB CARD DISCLOSURE ACT OF 1999	6
H. COMMON LAW.....	7
1. <i>Tortious Invasion of Privacy</i>	7
2. <i>State Actions: Anonymity on the Internet</i>	7
III. FEDERAL – EXISTING LAW	8
A. PRIVACY ACT OF 1974 (1994 & SUPP II 1996)	8
B. CHILDREN’S ONLINE PROTECTION ACT (COPA) - 1998	9
C. CHILDREN’S ONLINE PRIVACY PROTECTION ACT OF 1998 (COPPA)	10
1. <i>General Provisions – 16 CFR Part 312</i>	10
D. GRAMM-LEACH-BLILEY ACT (P.L. 106-102)	12
1. <i>FTC Final Rule: Privacy of Consumer Financial Information</i>	12
E. NATIONAL LABOR RELATIONS ACT (NLRA ACT) - PROTECTING E MAIL --- “CONCERTED ACTIVITIES” .	13
F. FTC INTERNET PRIVACY ACTIONS AND INDUSTRY INITIATIVES.....	14
1. <i>Online Privacy Alliance (OPA)</i>	14
2. <i>Network Advertising Initiative (NAI): Online Profiling</i>	15
3. <i>FTC Cases</i>	16
IV. FEDERAL - PROPOSED RULES AND LEGISLATION	18
A. FEDERAL COMMUNICATIONS COMMISSION LOCATION-BASED PRIVACY GUIDELINES.....	19
B. MODEL STATE PUBLIC HEALTH PRIVACY PROJECT.....	19
C. PROPOSED LEGISLATION – 106 TH CONGRESSIONAL SESSION.....	20
1. <i>H.R.4585 Medical Financial Privacy Protection Act</i>	20
2. <i>HR 3560 Online Privacy Protection Act of 2000 ; S809 Online Privacy Protection Act of 1999</i> 20	
V. STATE OF CALIFORNIA - PROPOSED LEGISLATION	21
1. <i>SB 1822, SB106, Bowen. Employee Computer Records</i>	21
VI. EUROPEAN UNION	21
A. EUROPEAN UNION (EU) DIRECTIVE ON THE PROTECTION OF PERSONAL DATA 95/46/EC.....	21
1. <i>Select Requirements of the Directive</i>	21
2. <i>US Proposed Safe Harbor – EU Adopts Safe Harbor Principles with reservations</i>	22
3. <i>Status of Safe Harbor Principles</i>	24
4. <i>Organizations Registered on the Safe Harbor List As of December 8, 2000</i>	24
B. STATUS OF IMPLEMENTATION OF DIRECTIVE 95/46 WITHIN THE MEMBER STATES OF THE EU AS OF NOVEMBER 20, 2000.	25
VII. CANADA	27

A.	PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT	27
VIII.	PRINCIPALITY OF SEALAND.....	28
A.	HAVENCO AND THE PRINCIPALITY OF SEALAND.....	28
IX.	GOVERNMENT SURVEILLANCE: INTERNET TRANSMISSIONS	28
A.	UNITED STATES: CARNIVORE	29
B.	BRITISH SYSTEM: ECHELON	30
C.	RUSSIAN SYSTEM: DUAL SYSTEMS.....	30
X.	INTERNET PRIVACY INFORMATION LINKS	30
XI.	NOTES / COMMENTS	31
XII.	ABOUT THE AUTHOR	32

I. On line Privacy

Privacy is a hot issue for 2001. Concern over the sharing of large databases of personal information gathered through both visible and invisible means has caught the attention of state, federal and international governments, organizations, consumers and business. The ability to categorize, record, track and share virtually every click and stroke of an individuals online travel has created a need to balance our right to privacy, our desire to have an optimal personal internet experience, business' goals to target prospective consumers and the states' need to protect society generally.

The national communications network is continuing to make the dramatic shift from voice communications to data communication networks. Data surpassed voice in 1998 as the largest consumer of telecommunications capacity.¹ Business models for online spaces are created to promote provide visitors instantly with specific products and content they may want. these models utilize advanced personalization algorithms², strategies that hinge on gaining an in-depth understanding of your visitors and capturing, analyzing and reporting on visitors behavior.³

The Internet has drawn focus to the many public sources of information that already exist. Many of the public records, which have been available in paper form, required a great deal of effort to obtain. You had to make the trip to the local courthouse to review or copy court cases, filings, bankruptcy records, land records or you had to wade through reams of paper spreadsheets or log books to find a particular record. Business records were often dispersed among various physical locations and many file cabinets. Computer network technology and the Internet made information, including personal information, that is customarily selectively shared at an individuals discretion, much easier to search for, copy and find. It is more cost efficient to compile demographic information or an individual dossier with a computer doing the searching, sorting, compiling and reporting.

The public appears surprised at the transparency of data collection through the Internet. Cookies, small computer programs placed on a personal computer by a web site publisher, can collect information while an individual is online that can be sent back to the web site publisher. This information can include a PC identifying marker, the web sites an individual went to next, how long they stayed at each site or page (clicks), whether they made purchases or downloaded files, as well as other data. E-mail, potentially, can be intercepted at any interim server it passes, to be read, altered, stored or recorded for future retrieval. Files "deleted" on a PC leave remains that can be used to reconstruct the file, at a later date. The computer age has an edge on it now that says if you use a PC to connect to world via the Internet or to keep any discreet files, you cannot hide.

For a small fee, online investing companies can provide via e-mail a report on any individual based solely on your providing a first name, last name, city and state information such as: Name, Current & Former Addresses, Phone Numbers, Social Security Numbers, Property Ownership – Real Estate, Automobiles, Airplanes, Boats, Neighbors, Others Who Live Or Have Lived At The Same Principal Address and more.

The United States approach to privacy has been a combination of minimal federal legislation, state legislation and self-regulation. Following is a selection of statues, federal and the State of California,

¹ The Industry Standard, Nov. 13, 2000. Jonathan Weber, [The End of Voice](#).

² Advertising comments from YourCompass, Inc.

³ Advertising by buystream, Measure what matters 2000.

cases and the European Union approach of legislative regulation that has emerged regarding online privacy.

A. Personal Information or Personal Identifying Information – What is private information?

The primary area of concern in regulating privacy deal with the protection of “personal information” or “personal identifying information”.

You will find definitions that differ slightly in the existing law and proposed legislation.

Definitions from California laws include:

CALIFORNIA CODES: CIVIL CODE §1798.80 INFORMATION PRACTICES ACT OF 1977: DISPOSAL OF INFORMATION

“Personal information” means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.

CALIFORNIA CODES: CIVIL CODE §1748.10 & 1748.12

“Marketing information” means the categorization of cardholders compiled by a credit card issuer, based on a cardholder’s shopping patterns, spending history, or behavioral characteristics derived from account activity which is provided to a marketer of goods for consideration. “Marketing information” does not include aggregate data which does not identify a cardholder based on the cardholder’s shopping patterns, spending history, or behavioral characteristics derived from account activity or any communications to any person in connection with any transfer, processing, billing, collection, charge back, fraud prevention, credit card recovery, or acquisition of or for credit card accounts.

CALIFORNIA CODES: INSURANCE CODE §791.02

"Personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. "Personal information" includes an individual's name and address and "medical record information" but does not include "privileged Information."

"Medical record information" means personal information that:

(1) Relates to an individual's physical or mental condition, medical history or medical treatment, and (2) Is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian

"Privileged information" means any individually identifiable information that both:

(1) Relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual. (2) Is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual. However, information otherwise meeting the requirements of this division shall nevertheless be considered "personal information" under this act if it is disclosed in violation of § 791.13.

CALIFORNIA CODES: GOVERNMENT CODE §11015.5(D)(1)

"Electronically collected personal information" means any information that is maintained by an agency that identifies or describes an individual user, including, but not limited to, his or her

name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, password, electronic mail address, and information that reveals any network location or identity, but excludes any information manually submitted to a state agency by a user, whether electronically or in written form, and information on or relating to individuals who are users serving in a business capacity, including, but not limited to, business owners, officers, or principals of that business. (2) "User" means an individual who communicates with a state agency or with an agency employee or official electronically.

CALIFORNIA CODES: PENAL CODE §530.5: IDENTITY THEFT

"Personal identifying information" as used in this section, means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.

CALIFORNIA CODES: PENAL CODE §637.6

"Personal information" means any information that identifies a child and that would suffice to locate and contact the child, including, but not limited to, the name, postal or electronic mail address, telephone number, social security number, date of birth, physical description of the child, or family income.

CALIFORNIA CODES: WELFARE AND INSTITUTIONS CODE §219.5

a) No ward of the juvenile court or Department of the Youth Authority shall perform any function that provides access to personal information including, but not limited to, social security numbers, addresses, driver's license numbers, or telephone numbers of private individuals ...

II. California – Existing Law

A. California Constitution – Inalienable Rights: Privacy

In 1972, the California State Constitution added a privacy provision:

Article I. § 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness, and privacy.

A person's privacy right is considered an inalienable right that may not be violated by anyone. This includes state actions, individual actions and business actions. This privacy interest is self-executing and confers a judicial right of action on all Californians⁴. The California Supreme Court has stated that the privacy provision is directed at four principal "mischiefs":

- "Government Snooping" and the secret gathering of personal information;
- Overbroad collection and retention of unnecessary personal information by government and **business** interests;
- Improper use of information properly obtained for a specific purpose; and
- Lack of a reasonable check on the accuracy of existing record.

This individual privacy right held by Californians can only be intervened by a compelling interest.

⁴ White v. Davis, (1975) 13 Cal.3d. at p. 757, 120 Cal.Rptr 94, 533 P.2d 732.

The language of the election brochure further stated that the provision was meant to provide "effective restraints on the information activities of government and business. (California Voter Pamphlet, p. 26 (1972).)

Leading cases discussing the California Constitutional Privacy Right include:

- *White v. Davis*, (1975) 13 Cal.3d 757, 120 Cal.Rptr.94, 533 P.2d 732.
Surveillance by undercover police agents, who posed as students, enrolled in university classes, recorded, and monitored students and faculty's conversations to compile dossiers of personal information on individuals would constitute a prima facie violation of the explicit right of privacy.
- *Porten v. The University of San Francisco*, (1976) 64 Cal.App.3d 825, 134 Cal.Rptr. 839.

B. Information Practices Act of 1977⁵

CALIFORNIA CODES: CIVIL CODE §1798

Requires state and local agencies, among other things, to maintain in its records only that personal information, as defined,

- which is relevant and necessary to its governmental purpose;
- to maintain its sources of information;
- to maintain accurate, relevant, and complete records;
- to disclose personal information only under specified circumstances;
- to maintain records regarding the disclosure of personal information; and
- to allow individuals access to those records pertaining to them, except as specified, to provide for the amendment of those records.

The act also establishes civil remedies for its enforcement. §1798.53 provides for a civil cause of action

Personal information is defined § 11015.5(d) of the Government Code:

(1) "Electronically collected personal information" means any information that is maintained by an agency that identifies or describes an individual user, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, password, electronic mail address, and information that reveals any network location or identity, but excludes any information manually submitted to a state agency by a user, whether electronically or in written form, and information on or relating to individuals who are users serving in a business capacity, including, but not limited to, business owners, officers, or principals of that business. (2) "User" means an individual who communicates with a state agency or with an agency employee or official electronically.

1. Customer Records: Personal Information: Disposal

Signed by Governor Davis, Sept. 30, 2000.

Adds to the Civil Code Part 4 of Division 3 § 1798.80.

Business is required to take all "reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information, which is no longer to be retained by the business..."

⁵ CALIFORNIA CODES CIVIL CODE § 1798 - 1798.1

1798. This chapter shall be known and may be cited as the Information Practices Act of 1977.

1798.1. The Legislature declares that the right to privacy is a personal and fundamental right protected by § 1 of Article I of the Constitution of California and by the United States Constitution and that, all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:

(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

(b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

“Customer” means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

“Personal information” means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.

C. California Public Records Act.

Public Records Act, Govt. Code §6250 et seq., governs public access to records maintained by state and local public agencies.

6250. In enacting this chapter, the Legislature, mindful of the right of individuals to privacy, finds and declares that access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person in this state.

6254.21. (a) No state or local agency shall post the home address or telephone number of any elected or appointed official on the Internet without first obtaining the written permission of that individual.

D. Personal Information: Collection and Disclosure— The Office of Privacy Protection

Signed by Governor Davis Sept. 29, 2000. Adds Article 7 (commencing with § 350) to Chapter 4 of Division 1 of the Business and Professions Code.

Makes California the first state to create an Office of Privacy Protection within the Department of Consumer Affairs. The office’s purpose shall be protecting the privacy of individuals’ personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices in adherence with the Information Practices Act of 1977 (Title 1.8 (commencing with § 1798) of Part 4 of Division 3 of the Civil Code). The department shall commence activities under this article no later than January 1, 2002.

The bill would require the office to inform the public of potential options for protecting the privacy of, and avoiding the misuse of, personal information, as specified, and to make recommendations to organizations for privacy policies, as specified, among other things.

The office shall make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers.

- Ensuring that commercial and governmental records are maintained such that personal information about individuals is not released in violation of law.
- Acting as a nonbinding arbiter in disputes regarding the unlawful release of personal information gathered by commercial or governmental entities.
- Recommending any corrections or changes to a commercial or governmental record pursuant to an administrative proceeding.

- Adopting any regulations necessary to implement the above requirements.
- Authorizes any commercial or governmental record holder found by the ombudsman to have unlawfully released personal information to seek redress in the courts.

E. Consumer Credit Reporting: Medical Information

Signed by Governor Davis September 29, 2000. Amends § 1785 of the Civil Code

This bill would also prohibit a consumer-reporting agency from including medical information in a consumer credit report provided for insurance purposes in consumer credit reports.

F. Areias Credit Card Full Disclosure Act of 1986: Credit Cards; Marketing Information

Signed by Governor Davis Sept. 29, 2000. Operative: April 1, 2002. This bill amends the Civil Code § 1748.10 and 1748.12 -- "Areias Credit Card Full Disclosure Act of 1986".

Requires the credit card issuer to give the consumers an opportunity to opt out annually of having their personal information shared.

If the credit card issuer discloses marketing information concerning a cardholder to any person, the credit card issuer shall provide a written notice to the cardholder that clearly and conspicuously describes the cardholder's right to prohibit the disclosure to marketers of goods of marketing information concerning the cardholder, which discloses the cardholder's identity. The notice shall include a preprinted form by which the cardholder may exercise this right and shall advise the cardholder of a toll-free telephone number which the cardholder may call to exercise this right.

"Marketing information" means the categorization of cardholders compiled by a credit card issuer, based on a cardholder's shopping patterns, spending history, or behavioral characteristics derived from account activity which is provided to a marketer of goods for consideration. "Marketing information" does not include aggregate data which does not identify a cardholder based on the cardholder's shopping patterns, spending history, or behavioral characteristics derived from account activity or any communications to any person in connection with any transfer, processing, billing, collection, charge back, fraud prevention, credit card recovery, or acquisition of or for credit card accounts.

G. Supermarket Club Card Disclosure Act of 1999

An act to add Title 1.4B (commencing with § 1749.60) to Part 4 of Division 3 of the Civil Code, relating to personal information.

The act prohibits a club card issuer from requiring an applicant for a supermarket club card to provide a driver's license or social security account number as a condition of obtaining the card. The act would also prohibit a club card issuer from selling or sharing personal identification information regarding cardholders, except as specified. The bill would also set forth various applicable definitions, and make any violation punishable as "unfair competition" pursuant to specified provisions of the Business and Professions Code. The bill would provide that its provisions are to become operative on July 1, 2000.

"Marketing information" means the categorization of cardholders compiled by a club card issuer, based on a cardholder's shopping patterns, spending history, or behavioral characteristics derived from account activity which is provided to any person or entity for consideration. "Marketing information" does not include aggregate data, which does not identify a cardholder based on the cardholder's shopping patterns, spending history, or behavioral characteristics derived from account activity.

H. Common Law

1. Tortious Invasion of Privacy

Four distinct forms of tortious invasion of privacy⁶ have been recognized:

- a) Commercial appropriation of the plaintiff's name or likeness
Codified in California in 1971 at Civ.Code. §3344, subd. (a).
- b) Intrusion upon the plaintiff's physical solitude or seclusion
- c) Publicity which places the plaintiff in a false light in the public eye; and
- d) Public disclosure of true embarrassing private facts about the plaintiff.

2. State Actions: Anonymity on the Internet

A growing area of litigation is concerning anonymity on the Internet. In many states civil actions have been brought to gain discovery of the identity of "John Does" who anonymously posted critical comments on a message board or in a chat room. The law is clearly unsettled among the states in respect to whether the identity of anonymous net users must be revealed in order for a potential plaintiff to access whether a claim may be made against the "John Doe".

Issues to be consider are:

- First Amendment Rights of free Speech and the possible chilling effect if discovery is allowed before proof of an actionable claim?
- Does the anonymous user have a legally recognized expectation of privacy?
- Has the user agreement with the ISP created an expectation of privacy in all cases? in limited cases?
- Does the ISP owe the user a duty to provide notice or does the user agreement provide that notice will be given for any request?
- Is the John Doe an employee, who has violated an employee agreement, revealed trade secrets, or violated another corporate policy for which disciplinary action may be available?
- Does the potential plaintiff have another means, than a court ordered disclosure, to identify the potential defendant?

1. **California: Columbia Ins. Co. v. Seescandy.com**, 185 F.R.D. 573 (N.D. Cal 1999). The court found they must balance the need to provide injured parties with a forum to seek redress for grievances and the traditional reluctance for permitting filings against John Doe defendants. The court went on to state:

However, this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously. People permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.⁷

⁶ Prosser, Torts (4th ed.) §117, pp. 804-814, see also Porten v. The University of san Francisco, 134 Cal.Rptr. 839.

⁷ As cited in Dendrite International v. John Does, et als. Docket No. MRS C-129-00, Nov. 23, 2000.

The court states a four-part test that must be met in order to discover the actual identity of the defendant:

- a. Identify the missing party with sufficient specificity such that a court can determine that the defendant is a real person or entity who could be sued in federal or state court;
 - b. Identify all previous steps taken to locate the elusive defendant;
 - c. Establish, to the court's satisfaction, that plaintiff's suit could withstand a motion to dismiss; and
 - d. File a statement of reasons justifying the specific discovery requested, as well as the identification of a limited number of persons or entities on whom the discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about the defendant that would make service of process possible.
2. **New Jersey: *Dendrite Int'l v. John Does, et al.***, Docket No. MRS C-129-00, Nov. 23, 2000.⁸

In possibly the only case to date denying the identification of such defendants, a New Jersey state court judge utilized the four-part test of *Seescandy.com*. In *Dendrite, supra*, the judge upheld the anonymity of two posters but ruled *Dendrite* could subpoena Yahoo! for the identities of the two other posters who did not challenge the subpoenas.⁹

III. Federal – Existing Law

A. Privacy Act of 1974¹⁰ (1994 & Supp II 1996)

Amended 1997, 5 U.S.C.A. §552(a)(West Supp. 1998), Effective: September 27, 1975
The Privacy Act is a codification of fair information practices. This law attempts to regulate the collection, maintenance, use and dissemination of personal information by federal government agencies. Subsection (v) requires the Office of Management and Budget (OMB) to (1) prescribe guidelines and regulations for the use of federal agencies in implementing the act; and (2) provide continuing assistance to and oversight of the Act by agencies. OMB guidelines are found at:

40 Fed. Reg. 28, 948-78 (1975)

40 Fed. Reg. 56, 741-743 (Supplemental Guidelines)

The policy objectives of the Act are:

- To restrict disclosure of personally identifiable records maintained by agencies;
- To grant individuals increased rights of access to agency records maintained on the individual;
- To grant individuals the right to seek amendment of agency records on themselves upon a showing that the records are not accurate, relevant, timely or complete;
- To establish a code of "fair information practices" which require agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

⁸ Superior Court of New Jersey, Chancery Division, Docket No. MRS C-129-00 See, <http://www.citizen.org/litigation/briefs/dendrite.pdf>

⁹ Yahoo!, Inc., privacy policy states that "...as a general rule, Yahoo! will not disclose any of your personally identifiable information except when we have your permission or under special circumstances..." Generally, Yahoo! will not release the identity of a user without a subpoena or court order.

¹⁰ See overview at www.usdoj.gov/oip/oip.html

Under the Act, an agency shall not disclose information to third parties without the individuals consent. There are twelve (12) exceptions to the consent rule:

- (1) "need to know to perform duties
- (2) disclosure pursuant to the Freedom of Information Act
- (3) Routine Use
- (4) Bureau of Census
- (5) Statistical Research
- (6) National Archives
- (7) Law Enforcement Request
- (8) Health or Safety of an individual
- (9) Congressional Committee or Subcommittee
- (10) Government Accounting Office
- (11) Court Order
- (12) Debt Collection Act (Consumer reporting agency)

The Computer Matching and Privacy Protection Act of 1998 (Pub. L. No. 100-503 and 101-508) amended the Privacy Act to add several provisions. These provisions added:

- procedural requirements for agencies to follow when engaged in computer-matching activities;
- requirements to provide the individual subject of the matching an opportunity to receive notice and to refute adverse information before having a benefit denied or terminated;
- clarification of due process provisions found in subsection (p).

B. Children's Online Protection Act (COPA) - 1998

Pub. L. No. 105-277, 112 Stat. 2681 (1998) Codified at 47 U.S.C. §231.

Commercial web publishers that distribute material that is "harmful to minors" as measured by "contemporary community standards" are required under COPA to ensure minors (persons under the age of 17) do not access the harmful material on the website.

Currently there is a preliminary injunction enjoining enforcement of COPA. See, *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), affirmed *ACLU v. Reno*, 31 F. Supp. 2d 47 (E.D. Pa. 1999), affirmed U.S. Court of Appeals for the Third Circuit, No. 99-1324 (Opinion Filed June 22,2000).

The Third Circuit found that:

because the standard by which COPA gauges whether material is "harmful to minors" is based on identifying "contemporary community standards", the inability of WEB publishers to restrict access to their WEB sites based on geographic locale of the site visitor, in and of itself, imposes an impressive burden on constitutionally protected First Amendment speech.

The court reasoned that the Internet is virtually without the geographical boundaries that allow a community to set clear borders within which notice of permitted and acceptable conduct restrictions will be readily known to a business. This borderless scheme means any Web publisher would be subject to the most restrictive and conservative state's community standards in order to avoid

criminal liability. As technology advances and given recent testimony by Internet experts in YAHOO! France, this reasoning may not be valid for long.¹¹

C. Children's Online Privacy Protection Act of 1998 (COPPA)

15 U.S.C. 6501, et seq.

Federal Trade Commission (FTC) Rule12: 16 CFR Part 312 Effective April 21, 2000.

This Act protects children's privacy by giving parents the tools to control what information is collected from their children online. Under the Act's implementing Rule (codified at 16 CFR Part 312), operators of commercial websites and online services directed to or knowingly collecting personal information from children under 13 must:

- notify parents of their information practices;
- obtain verifiable parental consent before collecting a child's personal information;
- give parents a choice as to whether their child's information will be disclosed to third parties;
- provide parents access to their child's information;
- let parents prevent further use of collected information;
- not require a child to provide more information than is reasonably necessary to participate in an activity; and
- maintain the confidentiality, security, and integrity of the information.

1. General Provisions – 16 CFR Part 312.

a) Personal Information

Definition includes: a first and last name, a home or other physical address, an e-mail address or other online contact information, including but not limited to an instant messaging user identifier or a screen name that reveals an individual's e-mail address, a telephone number, a social security number, a persistent identifier such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information, or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition. §312.2(a)-(g).

b) Privacy Notice on The Web Site §312.3(a)

An operator who collects any personal information from a child must provide notice on the web site or the online service of what information it collects from children, how it uses such information, and its disclosure practices for such information. This notice must comply with §312.4(b), which requires:

- notices to be clearly and understandably written, be complete, and must contain no unrelated, confusing or contradictory materials;
- a link to a notice of its information practices on its homepage and at each area on the website or online service where personal information is collected from children;
- the link must be in a clear and prominent place in each required area;
- the notice must state the name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the web site or online service;

¹¹ In November 2000, French Judge Gomez ruled that ruled that Yahoo must put a three-part system in place that includes filtering by IP address, the blocking of 10 keywords and self-identification of geographic location. The system follows the recommendations of an expert panel appointed by the court to investigate such technologies, which revealed its findings earlier this month. Yahoo will have three months to put the system in place, after which time the company would be subject to a fine of 100,000 francs (\$13,000) a day if the system has not been implemented.

¹² Copies of all FTC Rules and comments are available at www.ftc.gov. The website home page includes a link to the FTC Privacy Initiatives page.

- the notice must state the types of personal information and whether it is collected passively (i.e., through cookies) or directly;
- how the personal information is to be used by the operator; and
- whether the information is disclosed to third parties, the nature of the third parties business, whether the third party has agreed to maintain confidentiality, security and integrity of the personal information; and
- procedures and methods for parents to review, delete and refuse to permit further collection or use of the child's information.

c) Verifiable Parental Consent §312.5

An operator must make reasonable efforts to obtain verifiable parental consent, taking into account available technology.

(1) Methods to obtain verifiable parental consent include:

A written consent form signed by the parent and returned via fax or postal mail, use of a credit card in connection with a transaction, having a parent call a toll free number staffed by trained personnel, using a digital certificate that uses public key technology, or using e-mail accompanied by a PIN or password obtained through one of the other verification methods.

d) Choice Regarding Disclosures to Third Parties

Parents have the option to consent to the collection and use of their child's personal information without consenting to the disclosure of information to third parties. §312.4(b)(vi). Also, see §312.6

e) Online Activities for Which Parental Control Is Not Required

§312.5(c) provides exceptions to prior parental consent::

- where the sole purpose of collecting the name or online contact information is to obtain parental consent or providing notice under §312.4;
- where the operator is responding to a one time request to a specific request from a child;
- where the personal information collected is not used by the operator for any other purpose than responding directly to a specific request of the child; or
- where the operator collects personal information to extent reasonably necessary to protect the safety of a child participant on the website

f) Coverage of Information Submitted Online

The Federal Register notice accompanying the rule makes clear that the rule covers only information submitted online, and not information requested online but submitted offline.

g) Role of Schools in Obtaining Consent of Students

The Federal Register notice accompanying the rule makes clear that schools can act as parents' agents or as intermediaries between web sites and parents in the notice and consent process.

h) Safe Harbor Program

In order to encourage active industry self-regulation, the Act also includes a "safe harbor" provision allowing industry groups and others to request Commission approval of self-regulatory guidelines to govern participating websites' compliance with the Rule.

D. Gramm-Leach-Bliley Act (P.L. 106-102)

1. FTC Final Rule¹³: Privacy of Consumer Financial Information

16 CFR Part 313 Effective November 13, 2000. Requires full compliance by financial institutions by July 1, 2001

The purpose of the Gramm-Leach-Bliley Act (G-L-B Act) is to enable an individual to limit the sharing of non-public information by a financial institution with a non-affiliated third party. The G-L-B Act requires financial institutions as defined by § 4(k) of the Bank Holding Company Act, to offer consumers and customers the opportunity to “opt-out” of the transmission of non-public personal information by the institution to non-affiliated parties.¹⁴

Sec 503(a) requires a financial institution to disclose its policies and practices with respect to sharing information both with affiliated and non-affiliated third parties to customers. The rules promulgated by the Federal Trade Commission (FTC) (16 CFR Part 313) applies only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes.¹⁵

a) Notices of the institutions privacy practices and policies:

- (1) must be made at the time of establishing a customer relationship with the individual and thereafter, as long as the relationship continues, on an annual basis to all customers¹⁶;
- (2) notice to consumers, who are not customers, must be made prior to disclosing non-public personal information to a non-affiliated third party, §313.4(a)(2);
- (3) accurately reflect the institutions privacy practices and policies, 16 CFR §313.6(a)(8);
- (4) must be clear and conspicuous, 16 CFR 313.3(b)(1), and
- (5) include a description of the opt-out rights and methods to opt-out that are available to the customer. 16 CFR 313.6(a)(6).

b) Online / Internet Requirements of the Rule:

(1) Disclosures on Web Pages:

§ 313.3(b)(2)(iii) provides that may be found to comply with the rule that they be “clear and conspicuous”, if they use text or visual cues to encourage scrolling to view the entire notice and ensure that other elements of the web page do not distract attention away from the notice. The financial institution must also place a notice of conspicuous link on a page frequently accessed by consumers, such as the page on which transactions are conducted.¹⁷

¹³ Complete copies of the Rule and comments can be found at www.ftc.gov

¹⁴ 16 CFR §313.1 Purpose and Scope;

¹⁵ Id.

¹⁶ 16 CFR §313.4(a)(1) Initial notice to consumers required; §313.5(a)(1) Annual notice to customers required; General rule.

¹⁷ FTC supplementary information report to final privacy rule, 16 CFR 313: Privacy of Consumer Financial Information, Page 15-16, and 16 CFR 313.3(b)(1) – 313.3(b)(2)(iii)

The financial institution must also place a notice of conspicuous link on a page frequently accessed by consumers, such as the page on which transactions are conducted.¹⁸

c) Online Institutions:

Institutions operating online, as well as those operating offline, will have to evaluate whether they are required to make disclosures, including (1) whether they are engaged in a financial activity, and (2) if so, whether they have consumers or customers that trigger the disclosure or other requirements of the act.

The FTC notes that one of the financial activities incorporated by reference into Sec. 4(k) of the Bank Holding Company Act is:

"providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if...[t]he data to be processed or furnished are financial, banking, or economic..."

12 CFR § 225.28(b)(14).¹⁹ Some financial software and hardware manufacturers, as described at may find themselves classified as financial institutions. However, if these manufacturers only sell to businesses they will have no disclosure obligations. In addition, this language, according to the FTC supplemental information brings into the definition of financial institution Internet companies that provide an individual with access via the company's web site, to the individual's financial accounts (such as credit cards, mortgages, and loans) by compiling, or aggregating the individual's on-line financial accounts.²⁰

d) Delivering privacy and opt out notices

Each customer can reasonably be expected to receive actual notice in writing, or, if the consumer agrees, electronically. 16 CFR §313.9(a) How to provide notices. It can be reasonably expected that a consumer who conducts transactions electronically, will have been given actual notice if a clearly and conspicuously posted notice is on the electronic site, and the consumer is required to acknowledge receipt of the notice as a necessary step of obtaining the particular financial product or service. 16 CFR §313.0(a)(b)(1)(iii).

E. National Labor Relations Act (NLRA Act) - Protecting Email — “Concerted Activities”

Many companies have policies restricting the use of company e-mail systems to business communications. Courts have generally held that since employers own the computers and the networks on which e-mail is facilitated, they are free to monitor, intercept, read, and to set the rules

¹⁸ FTC supplementary information report to final privacy rule, 16 CFR 313: Privacy of Consumer Financial Information, Page 15-16, and 16 CFR 313.3(b)(1) – 313.3(b)(2)(iii)

¹⁹ Id., Page 36.

²⁰ Id., Page 36.

for use and the ramifications for misuse. Employees have no privacy rights in e-mail sent through a company e-mail system where an employer has provided notice to an employee of a policy that states the employer will monitor or intercept e-mail at their discretion.

However, taking a different cause of action, “unfair labor practices”, the NLRB found the e-mail protected. Messages the company found to be in violation of company e-mail policy and used as a basis for disciplinary action against employees were found to be “concerted activities” and protected by the NLRA Act. The e-mails were used to communicate about work terms and conditions. Thus, a complete ban is not always possible. The cases lend some guidance as to when an employer can ban all non-business use and discipline employees based on the content of monitored e-mail.²¹

1. NLRB v. Timekeeping Systems, 323 NLRB No. 30, Feb. 1997

In the NLRB’s first ruling that the use of e-mail is protected, when used by non-supervisory workers to communicate with other employees in an effort to influence working conditions, occurred in 1997. The NLRB concluded that the Timekeeping Systems, Inc. violated §8(a)(1) of the NLRB Act by discharging the employee, Larry Leinweber, for an e-mail that was transmitted to other employees and was, in and of itself, “concerted activity” within the meaning of the NLRB Act.

2. NLRB v. Pratt & Whitney – Advisory Memo

An employee of Pratt & Whitney, Brian Waldron, was suspended for one month without pay, in June 1997, after having “been warned, suspended or otherwise disciplined” for using e-mail for union messages or because employees have downloaded information from the union’s Web page onto company computers. Pratt & Whitney had a policy in place that banned the use of company computers and e-mail for all non-business uses.

The NLRB’s general office issued an advisory memo stating that a company cannot issue a complete ban on all e-mail, which necessarily includes employee’s messages otherwise protected by federal law. The memo included the analogy that e-mail was more like a telephone call than mail, as it allows the reader to talk back. The ability to exchange ideas and discuss what action to collectively take is the key to effective preservation of labor rights and the equalization of bargaining power.

While the advisory memo is not precedent, it does provide guidance to companies as they establish and review e-mail policies. Pratt & Whitney later changed the e-mail policy to allow for occasional personal use of company e-mail and to allow for discussions relating to the “terms and conditions of employment and the employee’s interest in self-organization.”

F. FTC Internet Privacy Actions and Industry Initiatives

1. Online Privacy Alliance (OPA)

The Online Privacy Alliance is a diverse group of more than 80 global corporations and associations who have come together to introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals’ privacy online. In the Spring of 1998, the Clinton Administration proposed to a group of business executives that if

²¹ Michael J, McCarthy, Wall Street Journal, *Workers new tool in privacy revolt*, as published in the San Francisco Examiner, Page J-1, May 21, 2000

internet companies could find a way to protect consumer privacy through self policing the federal government would leave them alone.²²

The guidelines the OPA developed were not universally adopted. The group's position has moved from whether congress will enact a new online privacy law to discussion of what the new law will look like. They are active in the development of a baseline privacy standard.

2 Network Advertising Initiative (NAI): Online Profiling

The Federal Trade Commission (FTC) has previously endorsed a self-regulatory program with limited legislative regulation. In July 2000, the FTC endorsed the Network Advertising Initiative (NAI) self-regulatory proposal that is aimed at addressing the privacy concerns consumers have with regard to online profiling.

NAI Principles:²³

a) Notice

Under the NAI Principles, consumers will receive notice of network advertisers' profiling activities on host Web sites and their ability to choose not to participate in profiling. Where personally identifiable information is collected for profiling, a heightened level of notice, "robust" notice will be required at the time and place such information is collected and before the personal data is entered. Where non-personally identifiable information is collected for profiling, clear and conspicuous notice will be in the host Web site's privacy policy. Under the NAI Principles, NAI companies will contractually require that host Web sites provide these disclosures and will make reasonable efforts to enforce those contractual requirements.

b) Choice

Once informed about the network advertiser's information collection practices, consumers should be able to decide whether to participate in profiling. Under the NAI Principles, the choice method depends on the type of information being collected and the consumer's knowledge about, and level of control over, the original collection of information. They provide that:

- Material changes in the information practices of a network advertising company, cannot be applied to information collected prior to the changes in the absence of affirmative (opt-in) consent of the consumer.
- Previously collected non-personally identifiable data ("click stream") cannot be linked to personally identifiable information without the affirmative (opt-in) consent of the consumer.
- "Robust" notice and opt-out choice (appearing at the time and place of information collection and before data is entered) is required for prospective use of personally identifiable information for profiling, including the merger of personally identifiable online and offline data.
- Clear and conspicuous notice and opt-out choice (appearing in the publishers' privacy policy with a link to the network advertiser or an NAI opt-out Web page) is required for prospective use of non-personally identifiable information for profiling.
- On sites where multiple network advertising companies collect information (generally non-personally identifiable information), consumers will be able to opt-out of profiling by any or all of the network advertisers on a single page accessible from the host Web site's privacy policy.

c) Access

²² The Industry Standard, Nov. 13, 2000, K. Washington, *The Persuader*.

²³ See, FTC at <http://www.ftc.gov/os/2000/07/onlineprofiling.htm#D.%20The%20NAI%20Principles>

Consumers will be given reasonable access to personally identifiable information and other information that is associated with personally identifiable information retained by a network advertiser for profiling.

d) Security

Consistent with the principle of Security, under the NAI proposal, network advertisers will make reasonable efforts to protect the data they collect for profiling purposes from loss, misuse, alteration, destruction, or improper access.

e) Enforcement

In a self-regulatory context, this means that nearly all industry members subject themselves to monitoring for compliance by an independent third party and to sanctions for non-compliance, which may include public reporting of violations or referral to the FTC. Enforcement may be provided by a seal organization, such as BBBOnline or TRUSTe.

Under the NAI Principles, network advertisers have committed to working with an independent third party enforcement program (e.g., a seal program) to ensure compliance with the Principles. If no such program is available within six months, the NAI companies will submit to independent compliance audits the results of which will be made publicly available.

f) Additional Consumer Protections

Finally, the NAI Principles provide additional protections for consumers beyond those required by the traditional fair information practices. For example, NAI companies will not use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, or social security numbers for profiling. In addition, NAI companies have committed to ensure that they obtain data for profiling from reliable sources.

NAI is a group of third party network advertisers who “are committed to increasing consumers confidence and contributing to the growth of electronic commerce.”²⁴ Members include: 24/7 Media, AdForce, AdKnowledge, Adsmart, Burst!Media, DoubleClick, Engage, Flycast, Matchlogic, NetGravity (a division of DoubleClick) and Real Media.

3. FTC Cases

a) FTC v. Toysmart.com, LLC, and Toysmart.com, Inc., July 2000

(District of Massachusetts) (Civil Action No. 00-11341-RGS).

The FTC settled the first case to be brought under COPPA by setting strict conditions for the sale of a database containing personally identifiable information of customers of Toysmart.com. Toysmart.com is a bankrupt web site, which holds as one of its most valued assets a database, including children’s personal information. It is the attempt to sell the database that drew the complaint from the FTC.

Detailed personal information contained in the database was collected pursuant to the Tysmart.com privacy policy. This policy stated that the information collected would never be shared with third parties. The sale would involve a “sharing”. The parties agreed the sale of the database could occur only if:

- The database shall not be sold as a stand-alone asset.
- Only to a "Qualified Buyer" may obtain the asset as part of an overall sale. A “Qualified Buyer” is an entity that is in a related market and that expressly agrees to be Toysmart.com’s successor-in-interest as to the customer information.

²⁴ See, www.networkingadvertising.org

- The Qualified Buyer must abide by the terms of the Toysmart.com privacy statement. If the buyer wishes to make changes to that policy, it must follow certain procedures to protect consumers. It may not change how the information previously collected by Toysmart.com is used, unless it provides notice to consumers and obtains their affirmative consent ("opt-in") to the new uses.
- In the event that the Bankruptcy Court does not approve the sale of the customer information to a Qualified Buyer or a plan of reorganization within the next year, Toysmart.com must delete or destroy all customer information.

b) Worldwidemedicine.com - Online Pharmacies

FTC v. Sandra L. Rennert, Philip Rennert, Lyle Mortensen, International Outsourcing Group, Inc., Focus Medical Group, Inc., Trimline, Inc., Affordable Accents, Inc., World Wide RX, Inc., World Wide Medicine, Inc., PSRenn, Inc., and Doctors A.S.A.P., Inc. (District of Nevada)

Operators of a group of Online pharmacies that promoted themselves touting medical and pharmaceutical facilities they didn't actually have and making privacy and confidentiality assurances they didn't keep, have agreed to settle Federal Trade Commission charges that their promotional claims were false and violated federal laws. The settlement with the promoters prohibits the deceptive claims; requires disclosures about medical and pharmaceutical relationships; bars the billing of charge cards without consumer authorization; prohibits disclosure of the information collected from consumers without the consumers' authorization; and, requires them to notify consumers of their practices regarding the collection and use of consumers' personal identifying information.

c) GeoCities, Inc., Aug 1998²⁵

GeoCities agreed to settle FTC charges that it misrepresented the purposes for which it was collecting personal identifying information from children and adults. This is the first FTC case involving Internet privacy. The case was settled before the COPPA rules implementation. Under the settlement, GeoCities agreed to post on its site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, GeoCities also would have to obtain parental consent before collecting information from children 12 and under.

d) Liberty Financial Companies, Inc. (younginvestor.com), May 1999²⁶

Addressing children's online privacy prior to COPPA, the FTC settled with Liberty Financial Companies, Inc., the operator of the Young Investor website. The Young Investor website is directed to children and teens, and focuses on issues relating to money and investing. The Commission alleged that the site falsely represented that personal information collected from children in a survey would be maintained

²⁵Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case: Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online, Aug. 13, 1998, <http://www.ftc.gov/opa/1998/9808/geocitie.htm>

²⁶ Young Investor Website Settles FTC Charges: Agency Alleged Website Made False Promises About Collection of Personal Information from Children and Teens, May 6, 1999, <http://www.ftc.gov/opa/1999/9905/younginvestor.htm>

anonymously, and that participants would be sent an e-mail newsletter as well as prizes. In fact, the personal information about the child and the family's finances was maintained in an identifiable manner. The consent agreement prohibits such misrepresentations in the future and would require Liberty Financial to post a privacy notice on its children's sites and obtain verifiable parental consent before collecting personal identifying information from children.

e) ReverseAuction.Com, Jan. 2000²⁷

Online auction house ReverseAuction.com, Inc. agreed to settle FTC charges that it violated consumers' privacy by harvesting consumers' personal information from eBay's site and then sending deceptive spam to those consumers soliciting their business. Settlement of the FTC charges' bar ReverseAuction from engaging in such unlawful practices in the future. It also requires ReverseAuction to delete the personal information of consumers who received the spam but declined to register with ReverseAuction; and to give those who did register, as a result of the spam, notice of the FTC charges and an opportunity to cancel their registration and have their personal information deleted from ReverseAuction's database.

f) DoubleClick, Inc. 2000 FTC Complaints and Pending Cases

On February 10, 2000, a complaint²⁸ was filed with the FTC alleging that the FTC notified DoubleClick that they were conducting an informal inquiry into DoubleClick business practices to determine whether, in collecting and maintaining information concerning Internet users, DoubleClick engaged in unfair or deceptive practices.

The complaint rises from the earlier purchase of Abacus Direct Corp. by DoubleClick. Abacus maintains one of the largest offline catalog databases in the country. DoubleClick proposed linking the anonymous Internet profiles in the DoubleClick database with the personal information contained in the Abacus database.

The complaint alleged that the merger of the databases violates DoubleClick's assurances to Internet users that the information it collects through their online activities will remain anonymous, and that the data collection is therefore unfair and deceptive.

DoubleClick also faced suits in various California jurisdictions²⁹. The allegations included improper collection and utilization of information about Internet users include unfair business practices, false and misleading advertising in violation of California consumer protection statutes, federal electronics privacy statutes, and common law privacy rights,

IV. Federal - Proposed Rules and Legislation

In the 106th congress, over 200 bills have been introduced that include some measures regarding privacy rights. It is expected that federal legislation will be introduced, with a significant chance of passage in the next session of congress. The legislation is expected to have support to establish

²⁷Online Auction Site Settles FTC Privacy Charges: Personal Identifying Information Hijacked From Competitor's Site; Many Consumers Sent Deceptive Spam, Jan. 6, 2000, <http://www.ftc.gov/opa/2000/01/reverse4.htm>

²⁸ Copies of the complaint can be found at www.epic.org/privacy/internet/ftc/CLK_complaint.pdf

²⁹ DoubleClick, Inc., February 14, 2000 SEC Edgar filing.

baseline privacy rights and expectations in line with the FTC's current four point standards: Notice, Access, Choice and Security.

A. FCC Location-Based Privacy Guidelines³⁰

The Federal Communications Commission (hereinafter, "FCC") received a "Petition From The Cellular Telecommunications Industry Association For A Rulemaking To Establish Fair Location Information Practices" in November 2000. The Cellular Telecommunications Industry Association (hereinafter, "CITA") , has proposed guidelines to direct carriers, manufacturers and third party vendors. pursuant to the Communications Act of 1934, as amended, §§222(f) & (h).

- Notice: provide each customer about the collection and use of location information;
- Consent: Provide each customer with a meaningful opportunity to consent to the collection before the information is used;
- Security and Integrity: ensure the security and integrity of any data collected.
- Access: permit the customer reasonable access to the location information to ensure its accuracy; and
- Uniformity across locations and technologies: provide uniform rules and privacy expectations so consumers are not confused as they roam or use different location technologies.

B. Model State Public Health Privacy Project³¹

Sponsoring organizations: Centers for Disease Control and Prevention (CDC), Council of State and Territorial Epidemiologists (CSTE), Association of State and Territorial Health Officials (ASTHO), National Conference of State Legislatures (NCSL), and Georgetown University La Center (GULC).

The purpose of the Model State Public Health Privacy Act project is to develop a model state law [hereinafter the "Act"] addressing privacy and security issues arising from the acquisition, use, disclosure, and storage of identifiable health information by public health agencies at the state and local levels. The Act regulates the acquisition, use, disclosure, and storage of identifiable, health-related information by public health agencies without significantly limiting the ability of agencies to use such information for legitimate public health purposes.

§1-103. Definitions (12) "Protected health information" means any information, whether oral, written, electronic, visual, pictorial, physical, or any other form, that relates to an individual's past, present, or future physical or mental health status, condition, treatment, service, products purchased, or provision of care, and which (a) reveals the identity of the individual whose health care is the subject of the information, or (b) where there is a reasonable basis to believe such information could be utilized (either alone or with other information that is, or should reasonably be known to be, available to predictable recipients of such information) to reveal the identity of that individual.

³⁰ See, The World of Wireless Communications, News & Commentary at http://www.wow-com.com/news/ctiapress/body.cfm?record_id=907 ; Pike and Fisher, Internet Law and Regulation, at http://www.pf.com/cgi-bin/om_isapi.dll?clientID=446168&advquery=%5bGroup%20NEWS1386%5d&infobase=ilr&recordswithhits=on&softpage=ILRNews

³¹ See, <http://www.critpathorg.msphpa/privacy.htm>

Protected health information is deemed non-public information, which cannot be disclosed without the informed consent of the person who is the subject of the information (or the person's lawful representative) unless otherwise allowed via narrow exceptions stated in the Act.

C. Proposed Legislation – 106th Congressional Session

1. H.R.4585 Medical Financial Privacy Protection Act

Sponsor: Rep. James A. Leach (Introduced 6/6/2000)

To strengthen consumers' control over the use and disclosure of their health information by financial institutions, and for other purposes.

House Committee on Commerce granted an extension for further consideration. 12/5/2000 House preparation for floor.

2. HR 3560 Online Privacy Protection Act of 2000³² ; S809 Online Privacy Protection Act of 1999

Related Senate Bill: S 809 Online Privacy Protection Act of 1999 (Intro: 4/15/1999)
Last Action: 10/3/2000 – Hearings Held .Committee on Commerce, Science, and Transportation.

HR 3560 Online Privacy Protection Act of 2000 (Intro: 1/31/2000)

Last Action: 2/4/2000 - Referral to House Committee on Commerce, Subcommittee on Telecommunications, Trade, and Consumer Protection.

"To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes."³³

Online Privacy Protection Act of 2000 - Makes it unlawful for an operator of a Web site or online service to collect, use, or disclose personal information concerning an individual (age 13 and above) in a manner that violates regulations to be prescribed by the FTC. Such operators would be required to protect the confidentiality, security, and integrity of personal information it collects from such individuals. Requires such regulations to require such operators to provide a process for such individuals to consent to or limit the disclosure of such information.

Authorizes the States to enforce such regulations by bringing actions on behalf of residents, requiring the State attorney general to first notify the FTC of such action. Authorizes the FTC to intervene in any such action.

³² Short Title as introduced in the U.S. House of Representatives January 31, 2000. Sponsor: Rep. Rodney P. Frelinghuysen

³³ Official Title as introduced.

V. State of California³⁴ - Proposed Legislation

California is one of the most active states in privacy regulation. The 2001 legislative session is sure to continue proposing regulation of the privacy of personal information of the citizens of California.

1. SB 1822, SB106, Bowen. Employee Computer Records.

Both vetoed by Governor Davis, Sept. 30, 2000.

(1) Existing law requires employers, generally, to grant employees the right to inspect personnel files.

This bill would have prohibited an employer from secretly monitoring the electronic mail or other computer records generated by an employee. The bill would have provided that an employer who intends to inspect, review, or retain any electronic mail or any other computer records generated by an employee shall prepare and distribute to all employees the employer's workplace privacy and electronic monitoring policies and practices.

VI. European Union

A. European Union (EU) Directive on the Protection of Personal Data 95/46/EC³⁶

Effective October 25, 1998.

The European Union (EU) Directive on the Protection of Personal Data (the Directive) (Council directive 95/46/EC, 1995 O.J. (L.281)) was enacted in 1995. The Directive requires "Member States to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection..." through the enactment of national laws.³⁷ The EU approach to privacy requires member countries to enact national laws to protect personal data.³⁸

1. Select Requirements of the Directive

- a) Member countries must enact national laws to protect personal data (for status of national laws, see, next § IV.A.2);
- b) prohibited from restricting the free flow of data between member countries;
- c) must restrict the flow of such data to nonmember countries whose laws do not "adequately" satisfy the Directive's standards;
- d) all processing of data must be done "fairly and lawfully";
- e) the purpose for which the data is collected must be specified and legitimate;
- f) data must not be used for non-sanctioned purposes;
- g) the data collected must be relevant and not excessive in relation to the purpose;
- h) personal data may only be processed upon the subject's specific, informed, and unambiguous consent;
- i) exceptions to consent include:

³⁴ The status and copies of the text of all bills before the California State Legislature can be found online at: www.leginfo.ca.gov

³⁵ Introduced by Senator Bowen, February 18, 2000, Amended March 23, 2000.

³⁶ Information on complying under the Safe Harbor Agreement is available at <http://www.export.gov/safeharbor/>

³⁷ European Union (EU) Directive on the Protection of Personal Data (Council directive 95/46/EC, 1995 O.J. (L.281), Article 25 paragraph 1

³⁸ Proposed cover letter of Ambassador David L. Aaron requesting comments from organizations, March 17, 2000. www.ita.doc.gov/td/ecom/aaron317letter.htm

- (1) necessary to the performance of a contract;
 - (2) to comply with a legal obligation;
 - (3) to protect the vital interests of the subject;
 - (4) in the public interest or in the exercise of official authority of the processing party; or
 - (5) in the legitimate interest of the processing party or third parties to whom the data has been disclosed.
- j) the subject must be notified of the identity of the entity controlling the collection, the intended purpose of the collection, the third party recipients, when the collection is obligatory or voluntary, and the consequences of failing to provide information;
 - k) the subject must be given the right to access the data and to rectify incorrect information.
 - l) The subject must be given the right to object to the data being used for direct marketing; and
 - m) A level of security appropriate to the risks presented and the nature of the data must protect the data collected.³⁹

2 US Proposed Safe Harbor – EU Adopts Safe Harbor Principles with reservations

The European Commission adopted a Decision determining that an arrangement put in place by the US Department of Commerce known as the "safe harbor" provides adequate protection for personal data transferred from the EU. At the same time, the Commission has adopted similar Decisions concerning Switzerland and Hungary.

The European Parliament, in its resolution of July 5, 2000⁴⁰, expressed the view that the "safe harbor" arrangement needed to be improved as regards remedies for individuals in case of breaches of the Principles before the Commission found it offered adequate protection. The EU Commission put the Department of Commerce on notice as regards the Parliament's concerns by informing the US side that it would re-open the discussions to seek improvements if the Parliament's fears about remedies for individuals proved to be well founded.

Organizations come into the safe harbor by self-certifying that they adhere to these privacy principles. The decision to enter the safe harbor is voluntary. Organizations must comply with the principles and publicly declare they do so. Self-certification requires notification from the organization to the Department of Commerce.⁴¹

a) The Safe Harbor Principles⁴²

- (1) **Notice**: requires that individuals be informed about the purposes for which the organization collects and uses information about the individual. Notice must be clear and conspicuous and be provided
 - (a) when individuals are first asked to provide such information; or
 - (b) as soon thereafter as is practicable; and
 - (c) in any event before the organization uses the information or discloses it for the first time

³⁹J. Millstein, J. Neuburger & J. Weingart, Doing Business on the Internet: Forms and Analysis, §10.03[2]

⁴⁰ See,

http://www3.europarl.eu.int/omk/omnsapir.so/pv2?PRG=DOCPV&APP=PV2&LANGUE=EN&SDOCTA=14&TXLST=1&POS=1&Type_Doc=RESOL&TPV=PROV&DATE=050700&PrqPrev=PRG@TITRE|APP@PV2|TYPEF@TITRE|YEAR@00|Fi nd@%73%61%66%65%20%68%61%72%62%2a|FILE@BIBLIO00|PLAGE@1&TYPEF=TITRE&NUMB=1&DATEF=000705

⁴¹ Procedures and requirements to self-certify can be found at <http://www.export.gov/safeharbor/SafeHarborInfo.htm#>

⁴² See, <http://www.export.gov/safeharbor>

It is not necessary to provide notice when the disclosure is made to a third party that is acting as an agent to perform tasks on behalf of and under the instructions of the organization.

(2) **Choice**: requires that individuals be given the opportunity to opt out whether and how their personal information is disclosed to third parties.

(a) **Sensitive Information** requires that individuals opt in prior to disclosure to third parties.

(i) Sensitive information includes personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.

(3) **Onward Transfer**: personal information may only be disclosed to a third party consistent with the principles of Notice and Choice. When an organization has not provided choice and the organization wishes to transfer the data to a third party, it may do so if it ascertains that the third party

(a) Subscribes to the principles; or

(b) Is subject to the Directive; or

(c) Another adequacy finding; or

(d) Enters into a written agreement with the third party requiring the third party to provide at least the same level of privacy protection as is required by the relevant principles.

If the organization transferring the data complies with these requirements, it shall not be held responsible when a third party to which the organization has transferred information, processes it in a manner contrary to any restrictions or representations UNLESS the organization knew or should have known the third party would process it in such a manner and the organization has not taken reasonable steps to prevent or stop such processing.

Onward Transfer applies to agents performing tasks on behalf of and under the instructions of the organization.

(4) **Security**: Organizations creating, maintaining, or 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**: Personal information collected must be relevant for the purposes for which it is to be used. To the extent necessary for these purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

(6) **Access: Individuals must have**

(a) access to personal information about them that an organization holds; and

(b) be able to correct, amend or delete that information where it is inaccurate, EXCEPT

(i) where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question; or

(ii) the rights of persons other than the individual would be violated

(7) **Enforcement: Mechanisms for assuring compliance (minimum)**⁴³:

⁴³ Enforcement –Dept. of Commerce FAQ regarding enforcement:

Q.: How should the dispute resolution requirements of the enforcement principle be implemented, and how will an organization's persistent failure to comply with the principles be handled? Can be found at :

- (a) Readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved;
- (b) Follow up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and implemented as presented; and
- (c) Obligations to remedy problems arising out of failure to comply
- (d) Sanctions

3. Status of Safe Harbor Principles

The Safe Harbor List became operational in November 2000. It is a self-certification, voluntary registration. A checklist for joining can be found at: <http://www.export.gov/safeharbor/checklist.htm>.

4. Organizations Registered on the Safe Harbor List⁴⁴ As of December 8, 2000.

The organizations on this list have notified the Department of Commerce that they adhere to the safe harbor framework developed by the Department of Commerce in coordination with the European Commission. An organization's self-certification to the safe harbor list, and its appearance on this list pursuant to the self certification, constitute a representation to the Department of Commerce and the public that it adheres to a privacy policy that meets the safe harbor framework. Participation in the safe harbor framework and self-certification to the list are voluntary. An organization's absence from the list does not mean that it does not provide effective protection for personal data or that it does not qualify for the benefits of the safe harbor.

In order to keep this list current, a notification will be effective for a period of twelve months. Therefore, organizations need to notify the Department of Commerce every twelve months to reaffirm their continued adherence to the safe harbor framework.

Organizations should notify the Department of Commerce if their representation to the Department is no longer valid. Failure by an organization to so notify the Department could constitute a misrepresentation. An organization may withdraw from the list at any time by notifying the Department of Commerce. Withdrawal from the list terminates the organization's representation of adherence to the safe harbor, but this does not relieve the organization of its safe harbor obligations with respect to personal information received during the time the organization is on the safe harbor list.

If a relevant self-regulatory or government enforcement body finds an organization has engaged in a persistent failure to comply with the principles, then the organization is no longer entitled to the benefits of the safe harbor. In this case, the organization must promptly notify the Department of Commerce of such facts by either email or letter. Failure to do so may be actionable under the False Statements Act (18 U.S.C. 1001). That organization must also provide the Department of Commerce with a copy of the decision letter from the relevant self-regulatory or government enforcement body.

In maintaining the list, the Department of Commerce does not access and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the

<http://www.ita.doc.gov/td/ecom/RedlinedFAQ11Enforc300.htm>

⁴⁴ See, <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe%20harbor%20list!OpenDocument&Start=1>

erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.

	Organization	Certification Status	Compliance Status	Personal Data Covered
1	Adar International, Inc.	Current		off-line, manually processed data
2	Crew Tags Int'l	Current		off-line, on-line
3	Cybercitizens First	Current		On-line, off-line, human resources data
4	Decision Analyst, Inc.	Current		on-line
5	HealthMedia, Inc.	Current		off-line and on-line
6	Numerical Algorithms Group, Inc.	Current		off-line, on-line, manually processed data
7	Privacy Leaders	Current		off-line, on-line, human resources data
8	The Dun & Bradstreet Corporation	Current		Off-line, on-line, manually processed
9	The USERTRUST Network L.L.C.	Current		On-line, off-line, human resources data
10	TRUSTe	Current		Online, offline
11	USERFirst	Current		On-line, off-line, human resources data
12	USERTrust Inc.	Current		On-line, off-line, human resources data

B. Status of Implementation of Directive 95/46⁴⁵ within the Member States of the EU as of November 20, 2000.

Member State	State of legislative procedure	Next steps
Belgium	<p>Implementation Law passed by Parliament on 11.12. 1998, (O.J. 03.02.1999).</p> <p>Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998</p> <p>In Dec. 1999, a public consultation of the draft of the secondary legislation was launched via the internet.</p>	secondary legislation to be adopted.

⁴⁵ The European Union in the U.S.: http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm

Member State	State of legislative procedure	Next steps
Denmark*	Parliament passed the Act. No. 429 of 31.05.2000 on processing of personal data on 26.05. 2000. 'The Act on Processing of Personal Data (Act No. 429) of 31 May 2000' Entry into force: 01.07.2000.	
Germany*	Draft Bill adopted by Federal Government on 14.06.2000 and presented to the Parliamentary bodies. The Federal Data Protection Act will cover Federal public authorities as well as private sector. Five Länder (Brandenburg, Baden-Württemberg, Hessen, Nordrhein-Westfalen, Schleswig-Holstein) adopted new DPLs pursuant to the Directive. These acts apply to the public sector of the respective "Länder".	The Bundesrat presented an opinion on 29.9.2000 (BR-Drs. 461/00 (Beschluss). First Reading by the Deutscher Bundestag on 27.10.2000.
Spain	Implementation law adopted 13.12.1999 Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999). Entry into force: 14.01.2000.	
France*	The Government consulted the data protection authority (La Commission nationale de l'informatique et des libertés) on the pre-draft of the bill in July 2000.	Parliamentary discussions likely
Greece	Implementation Law 2472 adopted: 10.04. 1997. Protection of individuals with regard to the processing of personal data Entry into force: 10 4.1997	
Italy	Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996. Entry into force: 8.5.2000 Additional legal acts previewed by Act no. 676 of 31.12.1996 (in particular, the Legislative Decrees no. 123 of 09.05.97, no. 255 of 28.07.97, no. 135 of 08.05.98, no. 171 of 13.05.98, no. 389 of 06.11.98, no. 51 of 26.02.99, no. 135 of 11.05.99, no. 281 and no. 282 of 30.07.99 ; the Presidentials decrees No. 501 of 31.03.98, No. 318 of 28.07.99)	Parliamentary discussion about the renewal of the delegation to the Government to complete Law 675.
Ireland*	Draft bill considered by the Government in July 1998 in view of presenting it to Parliament	Bill to be approved by the Government and submitted to Parliament
Luxembourg*	A new DPL was submitted to Parliament beginning October 2000.	
The Netherlands	DPL approved by the Senate on 06.07.2000, (O.J. 302/2000). Personal Data Protection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000. Estimated entry into force: Spring 2001	Secondary legislation to be adopted.

Member State	State of legislative procedure	Next steps
Austria	Directive implemented by the Data Protection Act 2000. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 . DSG-2000) vom 17.08.1999 Entry into force: 1.01.2000. Adopted ordinances: Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), Federal Law Gazette II Nr. 521/1999, about countries with adequate DP legislation (Switzerland and Hungary); Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2000 - DVRV), Federal Law Gazette II Nr. 520/1999, about the registration procedure; and Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 - StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification.	
Portugal	Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecção de dados pessoais' Entry into force: 27.10.1998	
Sweden	Directive implemented by SFS 1998:204 of 29.4.98 and regulation SFS 1998:1191 of 03.09.98 Entry into force: 24.10.1998.	
Finland	The Finnish Personal Data Act (523/1999) was given on 22.4.1999 Entry into force: 01.06.1999.	
United Kingdom	Royal Assent given to Data Protection Act 1998 on 16.07.1998. Subordinate legislation passed on 17.02.2000. Entry into force: 01.03. 2000.	

* means that the Member State is subject to a Commission Decision to bring the Member State to the European Court of Justice for failure to notify the implementing measures within the deadline established by the Directive.

VII. Canada

A. Personal Information Protection and Electronic documents Act

Canada's personal Information Protection and Electronic documents act becomes law January 1, 2001. The act requires businesses to offer Canadian citizens certain guarantees regarding the collection and use of personal information.

VIII. Principality of Sealand

A. HavenCo and the Principality of Sealand

The Principality of Sealand⁴⁶, a second world war fortress off Felixtowe in Suffolk, is setting itself up as a 'data haven' for companies wishing to store electronic files outside the jurisdiction of UK e-commerce law (e.g. The Directive). 'Prince' Roy Bates and HavenCo are reportedly offering unregulated Internet trading for \$10,000 (£6,623) plus \$1,500 per month.

HavenCo, states that they are not trying to undermine the authority of other governments. HavenCo is simply promoting, in conjunction with the Government of Sealand, a Philosophy of Contract Autonomy, as opposed to the Philosophy of Regulation. They state on the HavenCo website:⁴⁷

Our belief is that individuals and groups engaging in unsavory activities will be publicly admonished in a world where communications are free. This includes distasteful actions by governments, corporations, organizations as well as individuals.

.....

We believe in the right of privacy, including the right to be left alone. We believe that individual freedom of communications, a central tenet in the United Nations' Declaration of Human Rights and the constitutions of many nations, means being able to communicate with and ONLY with whomever you choose. This is why we support pseudonymity, anonymity and the unrestricted use of encryption techniques and tools for all.

.....

HavenCo claims it will provide a place for secure eCommerce, privacy-protected Internet services and uncensorable free speech.

IX. Government Surveillance: Internet Transmissions

Many governments are devising methods and tools to monitor criminal activities and the communications between suspected criminals that are capable of transmissions such as email on the Internet. Searches and monitoring involving Internet communications are made pursuant to the following acts and others:

- U.S. Constitution 4th Amendment
- Electronic Communications Privacy Act
- Computer Fraud & Abuse Act
- National Infrastructure Protection Act
- Communications Assistance for Law Enforcement Act (CALEA)

⁴⁶ For information on the Principality of Sealand see, <http://www.sealandgov.com>

⁴⁷ HavenCo Frequently asked Questions: 7. Aren't you just trying to undermine the authority of the world's major governments? Found at http://www.havenco.com/about_havenco/faq.html#seven

Systems to monitor email are in development and active throughout the world. Below are a few examples:

A. United States: Carnivore⁴⁸

Carnivore is an automated system attached to an ISP's to record email under the direction of the Federal Bureau of Investigation (hereinafter, "FBI"). FBI documents have been released under the Freedom of Information Act (hereinafter, "FOIA"), reports that carnivore "could reliably capture and archive all unfiltered traffic" transmitted through an Internet service provider and store the communications on a hard drive or removable disks.

The FBI states at its Carnivore web site⁴⁹:

In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. This type of tool is necessary to meet the stringent requirements of the federal wiretapping statutes.

The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being transmitted either to or from the named subject.

...

The use of the Carnivore system by the FBI is subject to intense oversight from internal FBI controls, the U. S. Department of Justice (both at a Headquarters level and at a U.S. Attorney's Office level), and by the Court. There are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties. The system is not susceptible to abuse because it requires expertise to install and operate, and such operations are conducted, as required in the court orders, with close cooperation with the ISPs.

Carnivore serves to limit the messages viewable by human eyes to those that are strictly included within the court order. ISP knowledge and assistance, as directed by court order, is required to install the device.

The FBI claims the system captures traffic that is isolated by a software filter that "minimizes" collection and limits it to the particular information authorized for seizure in a court order. Privacy groups and Congress have found "skepticism" about Carnivore and whether this capability would be exploited to do more than just intercept narrowly targeted pieces of information.

⁴⁸ For further information and selected Carnivore documents released as part of Electronic Privacy Information Center's (EPIC) FOIA lawsuit, See: http://www.epic.org/privacy/carnivore/foia_documents.html

⁴⁹ See, FBI Carnivore Web Site at <http://www.fbi.gov/programs/carnivore/carnivore.htm>

An independent technical review of Carnivore has been released by a review team from the Illinois Institute of Technology and sanitized by for release by Justice Department officials. This report can be found at: http://www.usdoj.gov/jmd/publications/carniv_entry.htm⁵⁰

B. British System: Echelon

Automated global interception and relay system; Developed under US-UK Agreement of 1947 with US-NSA, UK, Canada, Australia & New Zealand

C. Russian System: Dual Systems

- a) Federal Security Service – Monitors Internet transmissions in and out of Russia
- b) Federal Agency for Government Communications and Information. Privacy Information

X. Internet Privacy Information Links

You can find more information on privacy issues at:

- Electronic Privacy Information Center <http://www.epic.org>
Washington D.C.
- Federal trade Commission <http://www.ftc.gov>
Washington D.C.
- Transatlantic Consumer Dialogue <http://www.tacd.org>
- Online Privacy Alliance <http://www.privacyalliance.com>
- Organisation for Economic Co-operation and Development (OECD) <http://www.oecd.org/dsti/sti/it/consumer>
- National Telecommunications and Information Administration <http://www.ntia.doc.gov/ntiahome/privacy/index.html>

⁵⁰ See, EPIC Alert vol. 7.21, Nov. 30, 2000 at http://www.epic.org/alert/EPIC_Alert_7.21.html

XI. Notes / Comments

XII. About the Author

Lynn M. Holmes

Attorney & Counselor-At-Law

P.O. Box 207, Forestville, Ca 95436

Phone: 707-887-9399 Fax: 707-887-8387 Email: lynn.holmes@usa.net

Lynn M. Holmes, Esq., is an attorney in private practice. Prior to private practice, she had a successful career in semiconductor industry, specifically in sales management, contract administration and international supply line management. She has worked for such companies as National Semiconductor and most recently, International Rectifier. In addition, Ms. Holmes was a principal in a manufacturer's representative organization and as a sales agent represented such companies as Philips Semiconductor, Level One Communications and Maxim Integrated Circuits.

Ms. Holmes practice is focused on legal issues for business development and transactions, corporations and the Internet. She assist businesses in obtaining, enforcing and protecting their intellectual property, including trade secret protection, copyright and trademark. She is an active member of the California State Bar Business Law Cyberspace Law Committee. With the committee, she has spoken at various bar meetings on the issues of Online Privacy and Web Agreements. In addition, she is a member of the Sonoma County Bar Association, American Bar Association and North Bay Multi Media Association.