OTHER MEDICAL RECORDS PRIVACY ISSUES:

- EU Privacy
- Privacy Litigation
- State Laws

June 10, 2001

The Second Annual Pharmaceutical Industry Regulatory & Compliance Summit

Arlington, Virginia

Kerry A. Kearney
412.288.3046
kkearney@reedsmith.com

Gary L. Kaplan
412.288.4268
gkaplan@reedsmith.com

Reed Smith LLP
435 Sixth Avenue
Pittsburgh, PA 15219

OTHER MEDICAL RECORDS PRIVACY ISSUES:

EU Privacy; Privacy Litigation; State Laws

TABLE OF CONTENTS

European Union Privacy

I. The EU Privacy Directive

A. **Why do U.S. pharmaceutical companies care about EU Privacy?** Pharmaceutical companies who import data from overseas must be aware of privacy requirements in the country which exports the data. Although many countries have now adopted privacy regulations applicable to the handling and export of personal data (e.g. Canada and Australia), the EEC regulations are the most complex and onerous. These EU privacy regulations apply to pharmaceutical companies' collection of information from employees who work overseas, as well as to personal data from adverse event reports, clinical trials and websites.

B. **European Community Directive on Data Protection** ("EU Privacy Directive") was adopted by fifteen countries of the European economic community ("EEC") on October 24, 1995. The EU Privacy Directive took effect October 25, 1998.

C. The EU Privacy Directive established principles for privacy protection and the free flow of data within the fifteen country EEC.

D. The Directive prohibits transfers of personally identifiable information to non EEC countries unless "adequate" privacy standards are observed. The Privacy Directive applies to personal data about EU nationals collected over the Internet by companies, no matter where those companies are located and may apply to every e-commerce company or website operator in the United States. The EU Privacy Directive provides the following definitions for personal data and the processing of personal data:

1. Personal data is defined as any information relating to an identity or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

2. The processing of personal data is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

E. The EU Privacy Directive provides:

1. Personal data must be processed fairly and lawfully.

2. Personal data must be accurate.

3. Data can only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

4. Personal data must be kept in a form which permits identification of the subject of the data for no longer than is necessary, for the purposes for which the data was collected.

5. Data subject must give unambiguous consent to the gathering and processing of personal data.

6. If consent was not obtained from the data subject, personal data cannot be processed.

7. Personal data revealing racial or ethnical origin, political opinions, religious or philosophical beliefs, trade union membership is entitled to heightened protection. The processing of data concerning health or sex life is prohibited.

8. Data subject has the right to object, on request and free of charge, to processing of personal data for marketing.

9. The processor of data must provide to the data subject:

   (a) the identify of the processor of the data;

   (b) the purposes of the processing;

   (c) the recipients or categories of recipients of the data;

   (d) the existence of the right of access to and the right to verify the data; and

   (e) that the personal data undergoing processing be identified as to its source.

F. Chapter 4 of the EU Privacy Directive provides for the transfer of personal data to third countries only if:

> "[T]he member states shall provide that the transfer to a third country of personal data which are undergoing processing or intended for processing after transfer may take place, only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this directive, the third country in question ensures an **adequate level** of protection. The adequacy of the level of protection afforded by a third country shall

be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." (emphasis added)

II. The EU Safe Harbor for U.S. Companies Who Import Personal Data from EEC

(See Information about Safe Harbor attached as Appendix A)

A. July 26, 2000: European Commission announced U.S. Department of Commerce "safe harbors" to provide adequate protection for personal data transferred from the EU to the U.S.

1. Under the "safe harbor," U.S. companies can voluntarily adhere to a set of data protection principles recognized by the EU commission as providing "adequate protection".

2. Participation in the "safe harbor" is optional, its rules are binding for those U.S. companies that decide to join.

3. Compliance with the "safe harbor" rules is backed by the law enforcement powers of the Federal Trade Commission. The EU Commission's adequacy finding on the "safe harbor" principals is binding on all fifteen member states.

4. The seven "safe harbor" principals are:

   1. Notice: Notice must be provided to the subject of the personal data before the organization may use the personal data for a purpose different from the reason for collection of the personal data and prior to its release to a third party. An organization must inform individuals:

   - About the purpose for which it collects and uses information about them.
   - How to contact the organization with any inquiries or complaints.
   - The types of third parties to which it discloses the information.
   - The choices and means the organization offers individuals for limiting its use and disclosure.

   2. Choice: Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. An organization must offer individuals the opportunity to choose (opt out) whether:

- Their personal information is to be disclosed to a third party.
- Their personal information is to be used for a purpose that is incompatible with a purpose for which it was originally collected.
- If the personal data contains 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, the subject of the information must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected.

3. **Onward Transfer:** To disclose information to a third party, organizations must ascertain that the third party subscribes to the safe harbor principles or is subject to the EU Privacy Directive or another adequacy finding.

4. **Security:** Organizations must take reasonable precautions to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. **Data Integrity:** Personal information must be relevant for the purposes for which it is to be used.

6. **Access:** Individuals must have access to their personal data and be able to correct, amend, or delete that information where it is inaccurate.

7. **Enforcement:** Effective privacy protection must include:

   - Readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are resolved.
   - Follow-up procedures for verifying that privacy practices are true and that privacy practices have been implemented as presented.
   - Sanctions must be sufficiently rigorous to ensure compliance.

5. Data transfers to U.S. companies that choose to remain outside of the "safe harbor" is possible, under other allowed exceptions (e.g. consent -- the data subject has given approval), or will require alternative safeguards such as a contract.

6. January 4, 2001: Only 30 U.S. companies had signed up for "safe harbor" treatment. Several U.S. trade organizations are recommending that members not seek "safe harbor" status. http://www.export.gov/safeharbor/SafeHarborInfo.htmq

7. The EC must review the safe harbor by November 1, 2001. European parliament members are reportedly upset that only 30 U.S. companies have signed up for safe harbor and have voiced concerns that privacy is not an important issue in the U.S.

III. EU Standard Clauses (attached as Appendix B)

A. On March 27, 2001, the European Commission voted to adopt standard clauses that should be included in contracts between any EC data explorer and any non-EC data importer. The standard clauses would permit transfer of personal data from EU states. These standard clauses will expose the data importer to suit in EU courts.

The standard clauses apply to any U.S. company that does not qualify under Department of Commerce safe harbor and to those companies who have no safe harbor (e.g., all financial services companies under Gramm-Leach-Bliley).

While standardized contracts provide a mechanism to keep the personal data flowing out of the EEC, they subject U.S. companies to the jurisdiction of courts in EU states and to their local laws. The standard clauses could also raise privacy standards that were agreed to in the safe harbor principles. The standard clause are more onerous.

B. Clause 4 of the Standard Clauses sets forth the obligations of the non-EEC data importer:

> "(a) that he [it] is not subject to mandatory requirements of the national legislation applicable to him restricting compliance with data protection principles beyond what is necessary in a democratic society to safeguard one of the grounds listed in Article 13 of Directive 95/46/EC;
>
> (b) to process the Personal Data in accordance with the set of principles attached to this contract ("Mandatory Data Protection Principles": annex ....) or;
>
> (c) if explicitly agreed by the data exporter, without prejudice to compliance with the purpose limitation, restrictions on onward transfers and the rights of access, rectification, deletion and objection mentioned in the "Mandatory Data Protection Principles", to process in all other respects the data in accordance with . . . :
>
> - the relevant legislation protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data applicable to a Data Controller in the country in which the Data Exporter is established, or,

- the relevant provisions found in any Commission decision under Article 25.6 of Directive 95/46/EC finding a third country to provide for adequate protection in certain sectors of activity only, provided that the data importer is based in that third country and not covered by these provisions.

* * *

(d) to deal promptly and properly with all inquiries relating to Personal Data:

(e) to submit at the request of the Data Exporter its data processing facilities for audit. The audit may be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the Data Exporter and, where applicable, in agreement with the Supervisory Authority;

(f) to co-operate with the Supervisory Authority the course of its inquiries and abide by the advice of the Supervisory Authority with regard to the processing of the data transferred;

(g) to make available to the Data Subjects upon request a copy of these Clauses and indicate the office handling complaints."

C. In turn, Clause 6 of the Standard Clauses provides that the data subject may sue the U.S. company which allegedly violates his/her privacy rights:

"(1) The Parties agree that Data Subjects who have suffered damage as a result of any violation of the standard contractual clauses are entitled to receive compensation from the parties for the damage suffered.

(2) The Data Exporter and the Data Importer agree that they will be jointly and severally liable for damage resulting from a breach of the obligations and/or conditions referred to in clause 3(1). In the event of a breach of these obligations and/or conditions, the Data Subject can take action before court against either the Data Exporter or the Data Importer or both.

(3) The Parties agree that they may be exempted from this liability only if they prove that none of them are responsible for the act incompatible with the obligations contained in these clauses. The Data Importer may also be exempted from liability if he proves that the Data Exporter is solely responsible for the act incompatible with the obligations contained in these clauses."

D. Clause 7 of the Standard Clauses provides that the data importer may be sued in the data subject's home country.

IV. Application of EU Privacy Directive to U.S. Drug Companies

A. Areas for Pharmaceutical Companies to Consider.

1. Adverse Event Reports.

2. Clinical Trials

3. Websites

4. Employee Information in Multinational Companies

B. Anonymous Data. In order to transfer data from the EEC, the data exporter should remove identifying data. For clinical trials, data export should be covered and consented to by the patient who agrees to participate in the clinical trial.

C. U.S. Website Operators. U.S. websites should include a "Privacy Policy" which:

1. includes the identity of the party which collects the data;

2. includes an outline of the personal data collected;

3. specifies the purposes for which the data is being collected, i.e., to process orders, to let the visitor know about other products/services provided by the business, etc.;

4. specifies party(ies) to whom the data may be disclosed (e.g., group businesses);

5. outlines steps the business takes to store data securely (optional);

6. explains use of cookies (e.g. "Cookies" are small prices of information stored by a browser on a computer hard drive which track the screens which a user views on a site. Cookies may collect personal information without the knowledge of the visitor.);

7. obtains the consent of users to collection and use of personal data in the manner specified by the business;

8. obtains the consent of users to transfer of personal information to countries outside the EEA; and

9. tells visitors that they can check their personal data on request (optional).

D. Transfer of Employee Information Outside the EEA to Related Companies. Employees can consent to the transfer of personal data out of the EC with the following language:

> "The Company holds personal data on all employees for general business purposes including administration and marketing. In particular, employees' personal data (including photographs) are held by the Human Resources Department and may be placed on the Company's computer network and website or in marketing literature. In the ordinary course of

the Company's business, such data may be sent to, or be accessible from, other countries which do not have laws to protect your personal data. You are deemed to acknowledge and accept all of these uses of data by working at the Company. If you have any objection to this use of your personal data by the Company, you should contact the Human Resources Manager immediately."

States' Privacy Enforcement Activities Against Pharmaceutical Company Promotions

I. State Enforcement Action Related to Patient Confidentiality

A number of states have sought to regulate pharmaceutical promotion -- and particularly manufacturer-sponsored incentives to promote the utilization of particular products -- through their consumer protection statutes. These laws generally prohibit unfair, deceptive trade practices. See generally D. Woodward, "Recent Multistate Enforcement Initiatives: Prescription Drug Promotional Practices," 50 Food & Drug L.J. 295 (1995). The states involved in the consumer fraud settlements involving manufacturer marketing programs have expressed four basic concerns:

- interference with the pharmacist's duty to provide independent professional judgment;
- nondisclosure of the pharmacist's financial interest to patients;
- untruthful claims in manufacturer-generated promotional materials; and
- preservation of patient confidentiality.
  See also "Prescription Sales, Privacy Fears," Washington Post (Feb. 15, 1998) at A1 (describing pharmacy chain "refill reminder" programs and third party sponsorship and administration).

A. State settlements involving Manufacturer Promotional Programs

1. American Cyanamid / Lederle Laboratories. In September of 1993, American Cyanamid entered into an "assurance of discontinuance / assurance of voluntary compliance" with five states concerning a 1992 promotional program relating to Lederle Laboratories "Prostep" smoking cessation patch. Under the "Pharmacists Educating Patients" program, Lederle paid pharmacists $2 for patient counseling and information gathering services each time a patient presented a prescription for Prostep, up to a maximum of $16. Based on the data, a consulting group retained by Lederle provided progress reports to participating pharmacies concerning the specific patients to whom Prostep was dispensed, as well as national outcomes reports without identifying information. Initially, patients were not advised that the information would be disclosed to the consulting group, but the

program forms ultimately were revised to disclose this fact and secure patient consent. The states alleged that the program amounted to a violation of statutes prohibiting unfair and deceptive trade practices insofar as it did not disclose the uses of the consumer data collected by pharmacies and the manufacturer's compensation to the pharmacist, as well as state statutes relating to disclosure of confidential patient information. Under the assurance, American Cyanamid was permitted to continue the program, provided that (i) the existence of any compensation paid to a pharmacist and the purposes and uses of any data collected from the patient would be disclosed to the patient, and (ii) it would submit written disclosure forms to FDA for approval. In addition, American Cyanamid agreed to pay each state $10,000.

2. Miles, Inc. In March of 1994, Miles, Inc. entered into an "assurance of discontinuance/assurance of voluntary compliance" with eleven states concerning Miles' promotional practices with respect to its product Adalat CC. In June of 1993, Miles proposed a "conversion program" under which it would pay pharmacists $35 for each consumer converted to Adalat CC from Procardia XL, a competing, non-bioequivalent product manufactured by Pfizer, Inc. As a result of a complaint from Pfizer, however, Miles did not implement the program. Instead, Miles implemented a "patient information program" under which it would pay pharmacists a $35 fee for cognitive and counseling services, based on written materials provided by Miles, with respect to each new prescription of Adalat CC. In order to receive the fee, pharmacists were required to provide information relating to the prescription (including the patient's name) to Miles. The states alleged that the program violated state statutes prohibiting unfair or deceptive trade practices, and promoted violations of state pharmacy practice laws prohibiting pharmacists from (i) disclosing confidential patient information and (ii) accepting remuneration to promote the sale of goods or services of the pharmacist or a third party. Under the settlement, Miles agreed to discontinue the program, to destroy consumer information in its possession acquired through the program, and to pay each state $55,000.

3. Upjohn. On August 1, 1994, eight states entered into an assurance of discontinuance with The Upjohn Company relating to promotional programs for Upjohn's oral antidiabetic product Glynase PresTab. Upjohn also manufactured Micronase, an antidiabetic product for which the patent had expired in 1992. Although Glynase was not bioequivalent to Micronase and other competing products, Upjohn's promotional materials contended that Glynase offered advantages over those products. Further, Upjohn initiated a variety of promotional programs, including a "Cognitive Services Reimbursement Program," under which Upjohn paid pharmacists for providing "cognitive services" to patients. Upjohn also entered into "contract programs" with pharmacy chains which contained one or more of the following features: (i) "fee-per-switch" payments; (ii) payments for telemarketing calls to "top Micronase physician prescribers"; (iii) payment for promotional mailings to consumers in the chain's data

base using Micronase or competitive drugs; (iv) payments for a drug intervention officer to contact patients using Micronase or competing products and their physicians; and (v) rebate payments based on shifts in market share. These incentives did not apply with respect to drugs dispensed to Medicaid patients. Upjohn specifically disputed the states' contentions that its promotional claims and the failure to disclose incentives to pharmacists were deceptive, but nevertheless provided a broad range of assurances under the settlement. These included assurances that Upjohn (i) would not pay remuneration to pharmacies to induce referrals or recommendations to purchase Glynase, (ii) would include specific statements concerning health risks and potentially increased medical costs in promotional materials recommending "switches," and (iii) would abide by specific limits on promotional claims regarding improved treatment or cost savings. In addition, Upjohn agreed to pay a total of $675,000 to the eight states involved.

B. Multistate Merck/Medco Settlement

On October 4, 1995, Merck and its PBM Medco Containment Services entered into an assurance of discontinuance with 17 states in connection with the solicitation of prescription changes through the PBM. Under the assurance, the companies are required to provide substantial disclosures to physicians and patients and to develop comprehensive compliance procedures in connection with pharmaceutical interventions. Specifically, the states objected to Medco pharmacists' failure to disclose the company's affiliation with Merck when contacting physicians and patients. In addition, Merck and Medco agreed to provide health plans with information disclosing the fact that enrollees' prescriptions may be subject to Merck and Medco's intervention programs, as well as all reasonably foreseeable uses of confidential patient information by the company. The settlement represents the first attempt to regulate PBM-initiated intervention programs directly, and may have broad implications for such programs, particularly when sponsored by manufacturer-affiliated PBMs.

Privacy Lawsuits

I. Suits Relating to Medical Privacy

A. Anonymous v. CVS Corp., No. 604804, (N.Y. Sup. Ct. 2001). Court found that CVS had violated privacy rights of pharmacy customers by transferring records without customer consent to new owner of pharmacy. Pharmacies have a fiduciary duty of confidentiality in prescription records, including AIDs records of the class representative plaintiff. CVS had acquired the records of at least 350 small pharmacies without customer consent. A ruling on the motion for class certification is pending.

B. Biddle v. Warren General Hospital, 715 N.E.2d 518, (1999). In 1999, the Ohio Supreme Court held that an independent tort exists for unauthorized,

unprivileged disclosure of nonpublic medical information obtained by counsel for a hospital, even when the disclosure was made to counsel who represented the hospital in a proceeding which required knowledge of the records.

C. Cossette v. Minnesota Power & Light, 188 F.3d 964, (8th Cir. Minn. 1999). The Eight Circuit interpreted provisions of the ADA (Americans with Disabilities Act of 1990 (ADA), 42 U.S.C. § 12101-12213) and held that the ADA protects employees from unauthorized disclosures of medical information by employers regardless of whether or not the employee is disabled.

D. D.K. v. Parents of D.K., No 4D00-3634 (Fla. Ct. Appeals 3/21/01). Florida parents in custody fight could not waive 17 year old daughter's privacy rights so as to gain access to her medical and psychiatric records in spite of the fact that state law allows the parent to act on behalf of the minor child in regard to care givers.

E. Darby v. Pharmatrak Inc., 00-CV11664, (D. Mass.2000). Class plaintiff charged that Pharmatrak secretly tracked his and other class members online actions at the sites of various drug employees in violation of federal and state privacy law, including the Electronic Communications in Privacy Act.

F. Doe v. Medlantic Healthcare Group Inc., No. 97-CA3889 (D.C.Super.Ct., 11/30/99). In 1999, the District of Columbia Superior Court awarded plaintiff $250,000 for a hospital's lack of adequate security measures in protecting patient medical records. Plaintiff's records and HIV status were accessed by a part-time, unauthorized employee and disclosed to plaintiff's co-workers. The court cited lax security, including the inability of the medical records software used by the hospital to trace and identify who had accessed the records.

G. Hirschfeld v. Stone, 193 F.R.D. 175 (S.D.N.Y. 2000) . Class certified of accused criminals whose psychiatric and medical records were made accessible to the public as part of the state's determination of who was fit to stand trial. Plaintiff prisoners claimed violations of their privacy rights under New York and federal law.

H. N.V.E. Pharm., Inc. v. Hoffman-La Roche, Inc., and Weld v. CVS Pharmacy Inc., 98-0897 (Mass. Super. Ct., Suffolk Co.). http://www.masslaw.com/masup/1007501.htm. A judge certified (and the appellate court affirmed) a statewide class action in a case accusing drugstore chain CVS Corp. of violating the confidentiality of customers' pharmacy records for financial gain in certain

"patient-compliance programs" in which CVS sent letters to its customers on behalf of drug companies. CVS and Elensys Care Services Inc., a direct-marketing company, agreed to send refill reminders and drug advertisements to CVS pharmacy customers. The mailings were sent on CVS letterhead but were paid for by the drug manufacturers whose drugs were advertised. The program was voluntarily discontinued because of bad publicity but the class actions continue.

I. Norman-Bloodshaw v. Lawrence Berkely Laboratory, 35 F.3d 1260 (9th Cir. 2000). Affirming settlement by the University of California of a class action which claimed that U. Cal. had violated 9,000 employees' privacy rights by testing workers without consent for genetic disorders, venereal disease and pregnancy. Further employee tests were banned under the settlement and money was paid to each class member.

J. Pharmatrak Inc. Communications Litigation, 2001 WL 64742. Six proposed class actions were consolidated alleging that collection of private data through the use of cookies for online visitors to pharmaceutical company websites violated user's privacy rights.

K. Scott v. Leavenworth Unified School Dist., 190 F.R.D. 583 (D. Kan. 1999). Magistrate judge in Kansas held that the ADA does not protect employees' medical information when discovery is necessary for a plaintiff to pursue an ADA claim.

L. Staples v. Rent-A-Center, No. C99-2987 MMC, (N.D. Ca., 2000) settlement approved 3/10/00. Approving settlement of a class action brought under California law alleging privacy and other statutory violations by a class of plaintiff job applicants and employees who were required to answer personal questions about sexual practices and beliefs in order to be considered for jobs or promotions. The tests were abandoned nationally by defendant as part of the settlement.

II. Court Actions Based On Alleged Violations Of Online Privacy

A. Amazon.com, Inc. In February, 2000, four class actions were filed against Amazon.com, Inc. and its subsidiary Alexa.Internet alleging that Alexa secretly intercepted electronic communications with computer software programs and sent the information to third parties including Amazon.com. Amazon.com acquired Alexa in June 1999. Alexa develops web navigation services that work with Internet browsers to provide information about the sites being viewed and to suggest related sites to the

user. Alexa's software can be downloaded by users to their computer and provides additional information about the websites that a user visits. Alexa software tracks and stores Internet usage paths when a user accesses a website. Complaints alleged violations of 18 U.S.C. §§ 2701, 2510 and common law invasion of privacy.

B. American Online, Inc. October, 1999: At the introduction of AOL released Version 5.0, two actions were filed against AOL alleging violations of privacy in this new 5.0 software.

C. Bidder's Edge, Inc. May, 2000: eBay.com sued Bidder's Edge, Inc., an internet-based aggregation site seeking an injunction preventing Bidder's Edge from accessing plaintiffs' computer system by use of automated querying. See eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000). Court granted injunctive relief to eBay finding that eBay.com had established that it faced irreparable system harm due to Bidder's Edge activities.

D. Chance v. Avenue A Inc., No. C00-1964C, (W.D. Wa 2000). Class plaintiff claimed that placement of cookies violated his privacy rights and for the site's failure to disclose the use of cookies in its privacy policies.

E. Chase Manhattan Bank, (New York Attorney General). In January 2000, the New York Attorney General's office won a settlement against Chase Manhattan Bank for selling personal financial information about its customers, including credit line limits and account balances to third party marketers. The information was used for telemarketing and direct mail solicitation of Chase customers. Chase received a commission on business transactions between the telemarketers and the customer.

F. Conboy v. AT&T Corp., (2nd Cir. In 2001). Affirming trial court's dismissal of complaint charging that AT&T had violated privacy right by transmitting and using information in plaintiff's long distance phone bills to collect credit card debt on customer's AT&T Universal credit card.

G. Coronado v. Bank Atlantic Bancorp., No. 99-12108, (11th Cir. 2000). Affirming dismissal of privacy class action against bank which turned over records under anti-money laundering statute, 31 U.S.C. 5318 and regulations. Class plaintiffs claimed that records were turned over to grand jury in violation of state and federal privacy laws.

H. DoubleClick, Inc. DoubleClick provides on-line advertising and "serves" banner ads to third party websites. When an Internet User accesses a website, the website's server sends a request via the user's browser to the ad service to send a banner ad to the user's computer. When serving an ad, DoubleClick collects non-personally identifiable information about Internet users who visit websites such as user's Internet Protocol address, browser type, date, time and whether the user clicks through a banner ad. DoubleClick uses these "cookie" files as part of its ad service delivery. DoubleClick Inc. Privacy Litigation, No. 00-Ciy-0641, (S.D.N.Y. 2001) In 13 consolidated lawsuits, Judge Naomi Reice Buchwald ruled that placement of cookies in banner ads does not violate federal law. The suits were filed when Double Click acquired Abacus and revised its privacy policy to warn that information gathered online might be associated with personally identifiable information.

I. Intuit Inc. March, 2000: A class action was filed against Intuit Inc. alleging that it intercepted personal and private information of users of Quicken.com and disclosed that information to third parties and that Quicken.com's site "contained a secret information-harvesting capacity" that was not disclosed to users.

J. iVillage. February, 2000: The Federal Trade Commission (FTC) in February, 2000 launched a review of healthcare Websites' privacy practices to determine whether personal information has been improperly shared. FTC action followed the California Healthcare Foundation's allegations that medical web-sites had shared personal data with third parties and failed to follow privacy policies. Websites contacted by FTC include: Health Central.com, and iVillage.com. Guidera, "FTC Reviews Privacy Issues at Health-Care Web Sites, "The Wall Street Journal, February 18, 2000.

K. Nationsbank. NationsBank was forced to pay more than $6.5 million to settle allegations that it provided its subsidiary NationsSecurities with customer names, financial statements and account balances in order to help the company sell closed-end bond funds to bank customers as their certificates of deposits matured.

L. Real Networks, Inc. RealNetworks produces an interactive media software package called RealJukebox that allows users to download, record and play music, either from the internet or from users' compact disks. See e.g., Bell v. RealNetWorks, Inc., CV-99-7376 (E.D.N.Y.). Complaints alleged violations of 18 U.S.C. §§ 1030, 2510 et seq. and 2701 et seq., and state claims of trespass, invasion of privacy, violation of unfair trade practices acts, unjust enrichment and violation of various consumer protection acts. On February 11, 2000, an Illinois court granted RealNetWorks's motion to stay the action pending arbitration under the license agreement. Lieschke v. RealNetWorks, Inc., 99C 7274,99 C 7389, 2000 U.S. Dist. LEXIS 1683 (N.D. M. February 11, 2000). See also, In re Reawemorky, Inc. Privacy Litigation, 00 C 1366, 2000 U.S. Dist. LEXIS 6584 (May 8, 2000).

M. Rivera v. MatchLogic Inc., No. 00-K-2289, (D. Co., 2000). Class plaintiff claimed that placement of cookies violated his privacy rights and for the site's failure to disclose the use of cookies in its privacy policies.

N. 32 Plaintiffs v. Bank of America, (D. Md. 2001). Bank of America was sued in a class action for selling unauthorized consumer credit reports to entities that were unaffiliated with the company in alleged violation of the Fair Credit Reporting Act (FCRA).

O. Toys R Us, Inc. August, 2000: Website users filed class actions against Toys 'R Us and Coremetrics for violations of the Electronic Communications Privacy Act regarding storage and interception of electronic communications and violations of the Computer Fraud and Abuse Act. See Zinman v. American Online, Inc., 00 Civ. 1019 (S.D.N.Y.); Drew v. American Online, Inc., Index 0. 00600931 (Sup. Ct., N.Y. Cty.). Plaintiffs alleged that Toys 'R Us failed to follow its own privacy policy which called for keeping personal information "completely confidential."

P. Yahoo, Inc. February, 2000: two actions were filed against Yahoo! Inc. and its affiliate Broadcast.com in Texas for violations of Texas anti-stalking law. See, e.g., Schiller v. Broadcast. com, Inc., et al, Civil Action No. 8-00CB78 (E.D. Tex).

Privacy State Laws and Preemption

A. HIPAA Preemption. More stringent state laws are not preempted by HIPAA. In the final privacy rule, HHS backed away from the proposed rule in which

HHS said it would provide guidance on which state laws are "more stringent" than the federal standard. HHS claims limited resources and that any HHS advisory opinions might not be followed by states.

B. How to Determine if a State Law is More Stringent. The exemption process in Section 160.204 of the privacy rule sets out a process for exception determinations for 'more stringent' state laws. The preemption standard is set forth in 160.203 which provides:

> "A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of state law preempts the provision of state law. This general rule applies, except if one or more of the following conditions is met:
>
> (A) A determination is made by the Secretary under § 160.204 that the provision of state law:
>
> (1) Is necessary;
>
> (i) To prevent fraud and abuse related to the provision of or payment for health care;
>
> (ii) To ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
>
> (iii) For state reporting on health care delivery or costs; or
>
> (iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
>
> (2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by state law.
>
> (b) The provision of state law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.
>
> (c) The provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation or intervention.
>
> (d) The provision of state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals."

C. State Privacy Laws. The most comprehensive analysis of state medical privacy statutes was undertaken in 1999 by the Health Privacy Project at Georgetown University. The report is available at http://www.healthprivacy.org.

D. In an effort to achieve some measure of uniformity, the Model State Public Health Privacy Project, operated by Georgetown University, released its Model State

Public Health Privacy Act in October, 1999. Model State Public Health Privacy Act with comments, as of October 1, 1999, www.critpath.org/msphpa/nodellaw5.htm.

Kerry A. Kearney
412.288.3046
412.288.3063 - FAX
kkearney@reedsmith.com

Gary L. Kaplan
412.288.4268
412.288.3063 - FAX
gkaplan@reedsmith.com

Reed Smith LLP
435 Sixth Avenue
Pittsburgh, PA 15219

June 10, 2001