Michigan
Law Revision Commission

THIRTY-FIFTH ANNUAL REPORT
2000

MICHIGAN
LAW REVISION COMMISSION

Term Members:

RICHARD D. McLELLAN, *Chairman*
ANTHONY DEREZINSKI, *Vice Chairman*
GEORGE E. WARD
WILLIAM C. WHITBECK

Legislative Members:

Senators:

BILL BULLARD, JR.
GARY PETERS

Representatives:

JENNIFER FAUNCE
LAURA BAIRD

Ex Officio Member:

DIANNE M. ODROBINA
Legislative Council Administrator
124 West Allegan, 4th Floor
P.O. Box 30036
Lansing, Michigan 48909-7536

Executive Secretary:

PROF. KEVIN C. KENNEDY
Michigan State University – Detroit College of Law
Law College Building
East Lansing, Michigan 48824

TABLE OF CONTENTS

This report may be downloaded from the Commission's Internet Web Site, http://www.milegislativecouncil.org/mlrcf.html

MICHIGAN LAW REVISION COMMISSION
Thirty-Fifth Annual Report to the Legislature
for Calendar Year 2000

To the Members of the Michigan Legislature:

The Michigan Law Revision Commission hereby presents its thirty-fifth annual report pursuant to section 403 of Act No. 268 of the Public Acts of 1986, MCL § 4.1403.

The Commission, created by section 401 of Act No. 268 of the Public Acts of 1986, MCL § 4.1401, consists of two members of the Senate, with one from the majority and one from the minority party, appointed by the Majority Leader of the Senate; two members of the House of Representatives, with one from the majority and one from the minority party, appointed by the Speaker of the House; the Director of the Legislative Service Bureau or his or her designee, who serves as an ex-officio member; and four members appointed by the Legislative Council. The terms of the members appointed by the Legislative Council are staggered. The Legislative Council designates the Chairman of the Commission. The Vice Chairman is elected by the Commission.

Membership

The legislative members of the Commission during 2000 were Senator Bill Bullard, Jr. of Highland; Senator Gary Peters of Bloomfield Township; Representative Jennifer Faunce of Warren; and Representative Laura Baird of Okemos. As Legislative Council Administrator, Dianne M. Odrobina was the ex-officio member of the Commission. The appointed members of the Commission were Richard McLellan, Anthony Derezinski, William Whitbeck, and George Ward. Mr. McLellan served as Chairman. Mr. Derezinski served as Vice Chairman. Professor Kevin Kennedy of Michigan State University-Detroit College of Law served as Executive Secretary. Gary Gulliver served as the liaison between the Legislative Service Bureau and the Commission. Brief biographies of the 2000 Commission members and staff are located at the end of this report.

The Commission's Work in 2000

The Commission is charged by statute with the following duties:

1. To examine the common law and statutes of the state and current judicial decisions for the purpose of discovering defects and anachronisms in the law and to recommend needed reform.

2. To receive and consider proposed changes in law recommended by the American Law Institute, the National Conference of Commissioners on Uniform State Laws, any bar association, and other learned bodies.

3. To receive and consider suggestions from justices, judges, legislators and other public officials, lawyers, and the public generally as to defects and anachronisms in the law.

4. To recommend such changes in the law as it deems necessary in order to modify or eliminate antiquated and inequitable rules of law, and to bring the civil and criminal law of this state into harmony with modern conditions.

5. To encourage the faculty and students of the law schools of this state to participate in the work of the Commission.

6. To cooperate with the law revision commissions of other states and Canadian provinces.

7. To issue an annual report.

The problems to which the Commission directs its studies are largely identified through an examination by the Commission members and the Executive Secretary of the statutes and case law of Michigan, the reports of learned bodies and commissions from other jurisdictions, and legal literature. Other subjects are brought to the attention of the Commission by various organizations and individuals, including members of the Legislature.

The Commission's efforts during the past year have been devoted primarily to three areas. First, Commission members provided information to legislative committees related to various proposals previously recommended by the Commission. Second, the Commission examined suggested legislation proposed by various groups involved in law revision activity. These proposals included legislation advanced by the Council of State Governments, the National Conference of Commissioners on Uniform State Laws, and the law revision commissions of various jurisdictions within and without the United States. Finally, the Commission considered various problems relating to special aspects of current Michigan law suggested by its own review of Michigan decisions and the recommendations of others.

As in previous years, the Commission studied various proposals that did not lead to legislative recommendations. In the case of certain uniform or model acts, the Commission sometimes found that the subjects treated had been considered by the Michigan Legislature in

recent legislation and, therefore, did not recommend further action. In other instances, uniform or model acts were not pursued because similar legislation was currently pending before the Legislature upon the initiation of legislators having a special interest in the particular subject.

In 2000, the Commission held extensive meetings on the Administrative Procedures Act of 1969. The Commission's work and recommendation to the Legislature will be issued as a special report in 2001. The Commission also studied the four topics listed below in 2000. The Commission recommends immediate legislative action on the second, third, and fourth topics.

The four topics are:

(1) Privacy and the Internet.

(2) The Michigan Sales Representative Statute.

(3) Recent Court Opinions Suggesting Legislative Action.

(4) Intervention of Prosecutors in Divorce Actions, MCL § 552.45.

Proposals for Legislative Consideration in 2001

In addition to its new recommendations, the Commission recommends favorable consideration of the following recommendations of past years upon which no final action was taken in 2000:

(1) Revisions to the Michigan "Lemon Law", 1995 Annual Report, page 7.

(2) Consolidated Receivership Statute, 1988 Annual Report, page 72.

(3) Condemnation Provisions Inconsistent with the Uniform Condemnation Procedures Act, 1989 Annual Report, page 15.

(4) Amendment of Uniform Statutory Rule against Perpetuities, 1990 Annual Report, page 141.

(5) Amendment of the Uniform Contribution among Tortfeasors Act, 1991 Annual Report, page 19.

(6) International Commercial Arbitration, 1991 Annual Report, page 31.

(7) Tortfeasor Contribution under Michigan Compiled Laws §600.2925a(5), 1992 Annual Report, page 21.

(8) Amendments to Michigan's Estate Tax Apportionment Act, 1992 Annual Report, page 29.

(9) Amendments to Michigan's Anatomical Gift Act, 1993 Annual Report, page 53.

(10) Ownership of a Motorcycle for Purposes of Receiving No-Fault Insurance Benefits, 1993 Annual Report, page 131.

(11) The Uniform Putative and Unknown Fathers Act and Revisions to Michigan Laws Concerning Parental Rights of Unwed Fathers, 1994 Annual Report, page 117.

(12) Amendments to the Freedom of Information Act to Cover E-Mail, 1997 Annual Report, page 133.

(13) The Uniform Conflict of Laws-Limitations Act, 1997 Annual Report, page 151.

(14) Amendments to MCL § 791.255(2) to Create a Prison Mailbox Rule, 1997 Annual Report, page 137.

(15) Uniform Unincorporated Nonprofit Association Act, 1997 Annual Report, page 144.

(16) Clarify whether MCL § 600.1621 invalidates pre-dispute, contractual venue selection clauses, 1998 Annual Report, page 203.

Current Study Agenda

Topics on the current study agenda of the Commission are:

(1) Declaratory Judgment in Libel Law/Uniform Correction or Clarification of Defamation Act.
(2) Medical Practice Privileges in Hospitals (Procedures for Granting and Withdrawal).
(3) Health Care Consent for Minors.
(4) Health Care Information, Access, and Privacy.
(5) Uniform Statutory Power of Attorney.
(6) Uniform Custodial Trust Act.
(7) Legislation Concerning Teleconference Participation in Public Meetings.
(8) Michigan Legislation Concerning Native American Tribes.
(9) Revisions to Michigan's Administrative Procedures Act and to Procedures for Judicial Review of Agency Action.

(10) Intergovernmental Agreements under the Michigan Constitution, Art III, § 5.
(11) Electronic Transactions.
(12) Termination of Parental Rights of Biological Fathers.

The Commission continues to operate with its sole staff member, the part-time Executive Secretary, whose offices are at Michigan State University-Detroit College of Law, East Lansing, Michigan 48824. The Executive Secretary of the Commission is Professor Kevin Kennedy, who was responsible for the publication of this report. By using faculty members at the several Michigan law schools as consultants and law students as researchers, the Commission has been able to operate at a budget substantially lower than that of similar commissions in other jurisdictions. At the end of this report, the Commission provides a list of more than 120 Michigan statutes passed since 1967 upon the recommendation of the Commission.

The Legislative Service Bureau, through Mr. Gary Gulliver, its Director of Legal Research, has generously assisted the Commission in the development of its legislative program. The Director of the Legislative Service Bureau continues to handle the fiscal operations of the Commission under procedures established by the Legislative Council.

The Commission continues to welcome suggestions for improvement of its program and proposals.

Respectfully submitted,

Richard D. McLellan, Chairman
Anthony Derezinski, Vice Chairman
William C. Whitbeck
George Ward
Senator Bill Bullard, Jr.
Senator Gary Peters
Representative Jennifer Faunce
Representative Laura Baird
Dianne M. Odrobina

A RESOLUTION HONORING REPRESENTATIVE LAURA BAIRD

A resolution to commend the Honorable Laura Baird.

Whereas, It is with great respect for her commitment to the highest standards in public service and the law that we honor and thank Representative Laura Baird as she completes her service as a lawmaker and member of the Law Revision Commission. Her respect for our system of self-government is a reflection of the insights, thoughtfulness, and vision she will now share with the people of this state as a circuit court judge; and

Whereas, Laura Baird, elected to the Michigan House of Representatives in November of 1994, brought her talents and energies to the Law Revision Commission on February 17, 1999. A graduate of Western Michigan University and Cooley Law School, she brought with her valuable experience in private practice and extensive experience in legal, health-related, and community boards and organizations. Her background as an Ingham County Commissioner also gave her a valuable perspective on the role laws play in all aspects of our society; and

Whereas, Representative Baird has contributed to the work of many legal organizations at the state and national levels, including the Michigan Sentencing Commission and the National Commission on Uniform State Laws. These experiences have enhanced her service to our state throughout her service as a legislator and earned her our respect; now, therefore, be it

Resolved by the membership of the Michigan Law Revision Commission, That we commend Representative Laura Baird for her service with the commission and wish her well in her judicial responsibilities.

A Resolution Honoring Representative Jennifer Faunce

A resolution to commend the Honorable Jennifer Faunce.

Whereas, It is with great respect for her professional and personal commitment to our state and its legal structure that we honor and thank Representative Jennifer Faunce for her service to the Michigan Law Revision Commission throughout the Ninetieth Legislature. This responsibility is symbolic of her devotion to the quality of Michigan's laws and her concern for the role that they play in shaping our society; and

Whereas, A graduate of Michigan State University and the University of Detroit School of Law, Jennifer Faunce came to the Capitol after her 1998 election by the people of her Macomb County community. Her legal experiences have included work in private practice and service as an assistant prosecuting attorney, as well as membership in numerous civic and legal groups; and

Whereas, The Michigan Law Revision Commission was created in the *Michigan Constitution of 1963* to examine Michigan's statutes and judicial decisions in order to advance the quality of our state's laws with needed reforms. The success of this notable effort is solely dependent upon the commitment of dedicated practitioners of the law like Representative Faunce. Her dedication to this concept in her work with the commission, as a lawmaker, and in all aspects of her career is deeply appreciated; now, therefore, be it

Resolved by the membership of the Michigan Law Revision Commission, That we extend this expression of our respect and thanks to the Honorable Jennifer Faunce, who served the commission from February 1999 to December 2000.

A RESOLUTION HONORING DIANNE M. ODROBINA

A resolution to honor and thank Dianne M. Odrobina.

Whereas, In appreciation of her variety of services on behalf of the Michigan Legislature and this state's legal system, we are pleased to commend and thank Dianne Odrobina. Her efforts on behalf of the Michigan Law Revision Commission as an ex officio member are symbolic of the commitment she has made to our state in several legal and administrative capacities; and

Whereas, Dianne Odrobina, a graduate of Michigan State University who earned a master's degree from the University of Detroit and a juris doctorate from Wayne State University, came to her position with the Michigan Law Revision Commission in 1996. At the time, she became the first Legislative Council Administrator, following the creation of the post by 1995 PA 189. Previously, Dianne had devoted herself to the legislative process as the Director of the Senate Majority Policy Office; and

Whereas, With experience as an assistant prosecutor in Wayne County, through the Macomb County Friend of the Court, and in private practice, Dianne Odrobina has a deep appreciation of the importance of consistency in our statutes. Her genuine understanding of the complexities of the law and her sincere belief in a sound legal framework as a vital contributor to our society reflect values that are important to Michigan's future; now, therefore, be it

Resolved by the membership of the Michigan Law Revision Commission, That we offer our thanks and best wishes to Dianne Odrobina in gratitude for her five years of service to this commission and her long and distinguished dedication to Michigan's legislative branch of government.

PRIVACY AND THE INTERNET:
A STUDY REPORT TO THE MICHIGAN LAW REVISION COMMISSION

TABLE OF CONTENTS

PRIVACY AND THE INTERNET: A GUIDE THROUGH THE LEGAL THICKET

"You already have zero privacy. Get over it." Scott McNealy, Chief Executive Officer, Sun Microsystems, Inc.

I. Introduction

The Internet is growing at a rate that outpaces any modern medium of communication.[1] Television took thirty-five years to reach thirty percent of households in the United States. The Internet's World Wide Web is expected to achieve this degree of market penetration a mere eight years after its popular debut. One recent study predicts that by the end of the year 2000 over 100 million Americans will be "surfing" the Web on a regular basis.[2] In comparison, at the end of 1998, 57 million Americans were utilizing the Internet.

In the Information Age, we leave extensive data trails, some initially anonymous, which can be linked to a person later. Congress recognized this point as early as 1974 when it enacted the Privacy Act.[3] This law broadly defines a "record about an individual" as "any item, collection, or grouping of information about an individual."[4] The Privacy Act further states that such a "record" can be an "identifying number, symbol or other identifying particular assigned to the individual."[5] The Privacy Act, despite notable flaws, represents the most comprehensive

---

[1] See U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY 4 (1998) ("The Internet's pace of adoption eclipses all other technologies that preceded it."). The legal literature on privacy and the Internet is vast – in fact, overwhelming. For a small sampling, see Eric Sinrod, Jeffrey W. Reyna & Barak D. Jolish, *The New Wave of Speech and Privacy Developments in Cyberspace,* 21 HASTINGS COMM./ENT. L.J. 583 (1999); Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet*, 26 HUM. RTS. 10 (1999); Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551 (1999); Joel R. Reidenberg. *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999); Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 COMPUTER LAW. 7 (1999); Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1 (1999); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information,* 74 WASH. L. REV. 1033 (1999).

[2] See Perry H. Roth, *Internet Industry*, Value Line, June 4, 1998, at 2219.

[3] 5 U.S.C. § 552a (1994).

[4] Id. § 552a(a)(4).

[5] Id.

attempt to structure information processing within the public sector.[6] It applies, however, only to federal agencies.

Types of personal data that may be disclosed on the Internet include user-supplied data (including name, e-mail address, social security number, credit card number), "clickstream" data (information logged by an Internet Service Provider to track its users' browsing history, including Web sites visited, purchases made, and advertisements viewed), cookies (small text files sent by a Web site to a user's computer which allow Web sites to track user preferences based on earlier visits), and information revealed by uniquely distinguishing features of a user's computer, such as the unique serial numbers contained in Intel's Pentium III chips. Currently, personal data on the Internet is protected in certain circumstances under various federal and state laws, including the Electronic Communications Privacy Act, the Federal Trade Commission Act, and the Privacy Act of 1974.

While the Internet serves as a tremendous resource for information, products, and services, this same technology also provides companies and individuals with the ability to collect information about Internet users and to distribute that information to others.[7] The Federal Trade Commission's 1998 report on Internet privacy, *Privacy Online: A Report to Congress*, states that 92 percent of commercial Web site operators surveyed collected personal information about visitors, but that only 14 percent actually disclosed to the visitors how the information is used.[8] Many Internet users understandably feel that this collection of data is an illegal invasion of privacy. They believe that such practices violate the users' rights to "information privacy," which is defined as the right of an individual to control the acquisition, disclosure, and use of personal information. Site operators argue that the collected information is a valuable commodity, and that they have the right to exploit it commercially. This argument is strengthened by the fact that the "postindustrial economy generally and the telecommunications sectors particularly are seeing increased competition ... [prompting] firms to exploit every competitive advantage, including the

---

[6] See PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 92 (1996); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999). For a list of Web sites with information on Internet privacy issues, see < http://www.gahtan.com/cyberlaw>.

[7] See Reno v. ACLU, 521 U.S. 844, 868-73 (1997) (describing some of the forms of on-line behavior); SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 186-209 (1995).

[8] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 4, 1998).

use of personal information."[9] After conducting its June 1998 survey, the FTC proposed a legislative model that identifies four elements necessary to protect consumer privacy on commercial Web sites: (1) provide notice to consumers on how their personal information is used; (2) give consumers a choice about whether and how their information is used; (3) provide security for personal information collected; and (4) allow consumers access to their own information to promote accuracy.

On July 1, 1999, the FTC issued a report entitled, *Self-Regulation and Privacy Online: A Report to Congress*, which reports that 93% of surveyed sites collect personal data from consumers, and 66% make some form of disclosure about the site's information practices. The 1999 Report acknowledges that the FTC's 1998 report, which was based on an extensive survey of over 1400 commercial Web sites, had concluded that "effective self-regulation had not yet taken hold" and had pointed toward the necessity of federal legislative solutions to protect consumers' privacy.[10] By contrast, the 1999 Report states that "[i]n the ensuing year, there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information."

The 1999 report discussed two industry-funded surveys conducted in March 1999. One involved 361 Web sites drawn from the 7,500 busiest servers on the Web; it found that 93 percent of the sites collected personal information, 66 percent posted at least one disclosure, and 44 percent posted privacy policy notices.[11] The second survey examined the top 100 Web sites; it found that 99 percent collected personal information, 93 percent provided at least one disclosure about their information practices, and 81 percent posted privacy notices.[12] The Commission noted that only 10 percent of sites in the larger survey and 22 percent of sites in the top 100 survey complied with all four substantive fair information practice principles.[13] Nevertheless, the Commission considered the survey results to be "real progress." Also encouraging were the Online Privacy Alliance's issuance of guidelines, and new "privacy seal" programs started up by

---

[9] See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STANFORD L. REV. 1193, 1238 (1998).

[10] See FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (June 4, 1998).

[11] Georgetown Internet Privacy Policy Survey (1999), conducted by Professor Mary Culnan, McDonough School of Business, Georgetown University.

[12] Online Privacy Alliance, Privacy and the Top 100 Sites: A Report to the Federal Trade Commission (1999). This survey also was conducted by Professor Culnan.

[13] 1999 FTC Report at 7.

TRUSTe, BBBOnLine, and others.

Based on this activity, the 1999 report concluded that "legislation to address online privacy is not appropriate at this time."[14] This conclusion stirred some controversy. One of the commissioners dissented, and Representative Rick Boucher (D-Va.) declared that he was "appalled" that the FTC did not recommend legislation.[15]

The Commission did announce in the 1999 report comprehensive plans to monitor further developments in self-regulation. Among its planned activities are public workshops on "online profiling" and the use of tracking software, task forces on access and security, a joint educational program with the U.S. Department of Commerce, and a new online survey.

For some time a consensus has been emerging that privacy interests must be protected online. Whether a legislative or self-regulatory solution is appropriate is a matter of considerable debate.[16] In May, 2000, the FTC for its part weighed in on the side of government regulation. The Commission concluded that self-regulation is not working and recommended that Congress enact legislation which would give the FTC the power to effectively monitor privacy on the Internet.[17] From a survey conducted in early 2000, the Commission was convinced that industry efforts alone have not been sufficient. Because self-regulatory initiatives to date have fallen short short of broad-based implementation of effective self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders. While there will continue to be a major role for industry self-regulation in the future, the Commission has recommended that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online.

The legislation recommended by the Commission would set forth a basic level of privacy

---

[14] Id. at 12.

[15] *Electronic Commerce: FTC Can Find No Need for Congress to Pass Legislation to Protect Online Privacy*, 77 Antitrust & Trade Reg. Rep. (BNA) 58 (July 15, 1999).

[16] See JEFFREY P. CUNARD, JENNIFER B. COPLAN & GEORGE VRADENBURG, III, COMMUNICATIONS LAW 1999, 581 PLI/PAT 853 (Nov. 1999); Electronic Privacy Information Center, Report 94-1, Privacy Guidelines for the National Information Infrastructure: A Review of the Proposed Principles of the Privacy Working Group <http:www.epic.org/privacy/internet/EPIC_NII_privacy.txt>.

[17] See FEDERAL TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (May 2000), <htttp://www.ftc.gov/os/2000/05/index.htm#22>.

protection for consumer-oriented commercial Web sites. It would establish basic standards of practice for the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act. Consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online would be required to comply with the four widely-accepted fair information practices:

> **(1) Notice.** E Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it *(e.g.*, directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
>
> **(2) Choice.** E Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided *(e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities.
>
> **(3) Access.** E Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review, correct, and delete information.
>
> **(4) Security.** E Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.

It is not likely that Congress will take up this proposal until after the November elections.

II. The Transmission and Collection of Personal Data Over the Internet

As a user "surfs" the Internet, each Web site visited and each page viewed within a site are logged by the user's ISP. The ISP typically keeps a record of each user's e- mail communications and "click stream data," such as advertisements viewed and purchases made. Operators also record user activities using "cookie" technology that personalizes the site with the user's preferences, based on earlier visits to that site. Cookies are sent from a server to the user's hard drive during browsing sessions. The cookies label one's Web browser with an electronic serial number so that the originating site can then identify the user the next time he or she enters.

Personal information can be transmitted and collected over the Internet in three ways: (1) through personal computers, (2) through Internet service providers (ISPs), and (3) through Web sites.

A. Personal Computers

In connection with personal computers, information deleted from a personal computer is generally easily recoverable, whether from the machine's hard drive or elsewhere.[18] In addition, personal computers store information about Internet activities. Web browsers (Netscape Navigator or Microsoft Internet Explorer) use software protocols that create files about Web sites that have been visited.[19] Anyone with physical access to a computer can access these data either by looking at drop down files on the browser's location bar or by accessing the "History" menu item found on both Netscape Navigator or Microsoft Internet Explorer. Remote access to these files is possible from the Internet by exploiting security flaws in Web browsers.[20]

Accessing information off the Internet results in the recording of data in computer cache files. From the Web, it is possible to access cache files through "JavaScripts" and "Java applets" that permit the remote uploading of these files. Persons who access the Internet can also reveal confidences by their acceptance of "cookies." A "cookie" is a general mechanism which server-side connections can use both to store and retrieve information on the client-side of the connection.[21] Cookies represent an effort by organizations to monitor people's interest in their

---

[18] Monica Lewinsky's experience demonstrates how computer files can be deleted, but not destroyed. The Office of Independent Counsel's report to the House of Representatives includes e-mails and draft letters, including messages to President Clinton that Lewinsky never intended to send, which were recovered from deleted files on Lewinsky's computer. This recovery was possible because use of a "delete" button on a computer does not destroy the information, but merely hides it from view. See THE STARR REPORT: THE EVIDENCE 448-59 (Phil Kuntz ed., 1998)

[19] See BRIAN UNDERDAHL & EDWARD WILLETT, INTERNET BIBLE 124-26, 147 (1998).

[20] See BRYAN PFAFFENBERGER, PROTECT YOUR PRIVACY ON THE INTERNET 182-91 (1997); David S. Bennahum, *Daemon Seed: Old email never dies*, Wired, May 1999, at 100, 102. The Office of the Independent Counsel appears to have used such a software program in recovering, for example, drafts of documents that Monica Lewinsky wrote and then deleted from her computer's hard drive. See STARR REPORT EVIDENCE, *supra* note 8, at 431. See also Jerry Adler, *When E- Mail Bites Back*, NEWSWEEK, Nov. 23, 1998, at 45 (noting that in its investigation of Microsoft, the Justice Department has obtained "an estimated 3.3 million Microsoft documents, including megabytes of e-mail messages dating from the early 1990s--and is using them to contradict Gate's own videotaped testimony in the most significant antitrust case of the decade").

[21] See James N. Thurman, *Here's one `cookie' many consumers don't want*, CHRISTIAN SCI. MONITOR, at 2, April 18, 2000.

products and services through the covert gathering of personal data without their knowledge and consent. Generally, cookies allow Web sites to "tag" their visitors with unique identifiers so that they can be identified each time they visit the site. The information obtained by the cookies identifies users' e-mail addresses, the names of their browsers, the types of computers they use, the universal resource locators (URL) or Internet addresses, the duration of the users' contact with Web sites, the specific pages of the Web sites that are visited, and what electronic transactions are made. Logging on to a Web site, or even viewing an on-line ad, can load a cookie onto a user's hard drive. Information is then collected by marketers to better sell their goods and services. When an individual returns to this same site at a later date, her browser automatically sends a copy of the cookie back to the Web site; the data identify her as a previous visitor and allow the site to match her to details regarding her prior visit.[22]

B. Internet Service Providers

Access to the Internet generally requires an account with an ISP which is the entity that supplies Internet connectivity. ISPs obtain access to detailed, and sometimes highly sensitive, information about their customers' behavior on the Internet. ISPs can combine these data with profiling information, which their clients share with them, as well as with information purchased from direct marketing companies.[23] Many outside entities, both governmental and commercial, are increasingly seeking access to these rich databases of personal information.[24]

C. Web sites

Web sites are the third locus for the collection of personal information on the Internet. In July 1999, the FTC released an Internet privacy study carried out on its behalf by Mary Culnan of Georgetown University's McDonough School of Business.[25] According to the survey, up to

---

[22] See Netscape, *Cookies and Privacy Frequently Asked Questions* <http:// www.home.netscape.com/products/security/resources/faq.cookies.html> (explaining that "cookies can be used to store any information that the user volunteers").

[23] See Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1748-49 (1995) (noting how a systems operator at a university can monitor activities of students and faculty on the Internet).

[24] See Edward C. Baig, *Privacy*, BUS. WK., Apr. 5, 1999, at 84 ("Personal details are acquiring enormous financial value. They are the new currency of the digital economy.").

[25] FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (July 1999) (hereinafter FTC Self-Regulation Report) (available at <http:// www.ftc.gov/opa/1999/9907/-report-1999.htm/>); Georgetown Internet Privacy Policy Survey <http:// www.msb.edu/faculty/culnan/gippshome.html>.

eighty-five percent of Web sites collect personal information from consumers. The Georgetown Internet Privacy Policy Survey reveals many problems in cyberspace. First, it shows that less than ten percent of surveyed sites provided even a subset of basic fair information practices. Second, the study indicates that a high percentage of Web sites are collecting personal information. Other potential problems were outside the study's scope. To begin with, the study did not examine whether Web sites offered procedural and substantive rights, such as redress or enforcement policies. Moreover, as the Center for Democracy and Technology observed, the survey provides no information about whether companies are actually following the privacy policies that they promised.[26] Finally, the Georgetown Survey does not consider whether Web sites are allowing individuals to limit release of their personal data to affiliated enterprises. This last issue is of particular significance at a time when mergers and consolidations are almost daily events among Internet companies and between Internet and Real Space companies.

The Georgetown Survey's empirical work indicated that 65.7 percent of the sites in the sample posted "at least one kind of privacy disclosure." For the Chairman of the FTC, Robert Pitofsky, this single development was solid proof of "real progress." The FTC's Chairman assured Congress that the Georgetown study helped indicate that "self-regulation is working." The FTC itself argued that "self-regulation is the least intrusive and most efficient means to ensure fair information practices online." In contrast, FTC Commissioner Sheila Anthony stated that "(n)otice, while an essential first step, is not enough if the privacy practices themselves are toothless." At present, her judgment is decidedly in the minority.

In what ways do Web sites collect personal information? Web sites collect personal data through cookies, registration forms, and sweepstakes that require surrendering e-mail addresses and other information. Other invasions of privacy relating to Web sites involve archives of comments made on the "Usenet" or to "list servs", and deceptive promises that Web sites sometimes make about privacy practices.

The Usenet allows participants to post communications into a database that others can access. List servs are listings of names and e-mail addresses that are grouped under a single name. Sending messages to these areas may be creating a permanent record of one's opinions. Transcripts of contributions to both the Usenet and list servs are sometimes collected and archived, often without disclosure to participants and without restrictions on further use. One such catalogue of these comments, "www.deja.com," provides four different archives, including one for "adult" messages.

Web sites also make available information through Web-based reference sites. Web sites (e.g., "Dig Dirt," "WeSpy4U," and "Snoop Collection") sell medical histories, criminal justice

---

[26] See Center for Democracy and Tech., Behind the Numbers: Privacy Problems on the Web <http:www.cdt.org/privacy>.

records, educational accomplishments, unlisted telephone numbers, yearly income, bank balances, stocks owned, and a variety of other kinds of financial data.[27]

III. Issues Involving Personal Privacy and the Internet

The privacy issues connected with the use of the Internet include (1) e-mail monitoring in the workplace, (2) data collection, (3) personalization, (4) anonymity, and (5) invasion of privacy in non-workplace settings.

A. E-Mail Monitoring in the Workplace

If e-mail is not already the most frequently used means of communicating in the workplace, it is close to it and gaining on its only rivals -- face-to-face meetings and telephone conferences. According to a 1998 survey conducted by the American Management Association, 20 percent of companies monitor their employees e-mail, an increase of 5 percent from a similar 1997 survey.[18] As the years pass, it can be presumed that the numbers will be even higher.

What are some of the justifications for employer e-mail monitoring? They include the rights and needs of companies to protect their property and themselves from liability, particularly with respect to harassment suits. Do employees have a legitimate expectation of privacy with regard to e-mail and Internet use? One must examine the constitutional (in the case of public employers), statutory, and common law origins of privacy protection for employees, along with applicable case law that has explored privacy issues in the workplace, including e-mail monitoring.

The federal statutory framework in this area is limited to the Electronics Communications

---

[27] For a sampling of these sites and sales policies, see Dig Dirt Inc. <http://www.digdirt.com>; WeSpy4U.com <http://www.wespy4u.com>; Snoop Collection <http://www.spycave.com/spy.html>. For example, the Snoop Collection promises "for one low fee" to provide the "enchantment of finding out a juicy tidbit about a co-worker" or checking "on your daughter's new boyfriend."

For an FTC report on these traditional look up services, see FTC, Individual Reference Services: A Report to Congress < http:www.ftc.gov/bcp/privacy/wkshp97/-irsdoc1.htm>. Following the FTC's investigation, this industry made adjustments to its privacy practices. See FTC, Information Industry Voluntarily Agrees to Stronger Protections for Consumers, <http://www.ftc.-gov/opa/1997/9712/inrefser.-htm>.

[18] See Hall Adams, III, Suzanne M. Scheuing, & Stacey A. Feeley, *E-Mail Monitoring in the Workplace: The Good, the Bad, and the Ugly*, 65 DEF. COUNS. J. 32 (2000).

Privacy Act of 1986 (ECPA).[19] An expanded version of an old wiretapping statute, the ECPA covers interception of "electronic communication" and unauthorized access of stored electronic communications. Although there are few cases in this area, legal scholars expect that provisions of this act relating to stored data ultimately will be used to cover most disputes regarding unauthorized access of e-mail. A violation of the ECPA is serious and carries both civil and criminal penalties.

The central issue -- whether, under the ECPA, employees who send e-mail communications in the course of their employment have a reasonable expectation of privacy -- remains unresolved. Some trial courts have held that an employee does not have a reasonable expectation of privacy when e-mail messages are sent to others within the company. For example, in *Smyth v. Pillsbury Co.*,[20] the employer, a private company, provided e-mail accounts for its employees. The court refused to force the employer to honor its promise of e-mail confidentiality. Because systems operators at the workplace had access to employee e-mail, no employee had a reasonable expectation of privacy in his or her e-mail, according to the district court, notwithstanding the employer's promise of confidentiality.

Since there is not yet a definitive appellate court decision resolving the issue of employee expectations of privacy in e-mail, guidance must be drawn from scattered cases and the act itself. Courts have found certain exceptions to the ECPA, including instances where prior written consent has been given by a telephone user, allowing an employer to intercept telephone communications. This is arguably a very narrow exception, however, involving very strong facts demonstrating clear, express consent. Another exception under the ECPA is the interception of communications that are intended to be shared, such as communications posted on a company bulletin board. In such a case, the employee does not have a reasonable expectation of privacy.

Many businesses now require employees to sign disclosure statements that authorize a management review of all e-mail communications may be reviewed at the conclusion of their employment. Authorizing this disclosure would reduce, but not eliminate, an argument that there is employer liability to the employee for violating an expectation or right of privacy.

---

[19] Electronics Communications Privacy Act of 1986, codified at 18 U.S.C. §§ 2510-2521, 2701- 2711, 3117 & 3121-3127. See Micalyn S. Harris, *E-Mail Privacy: An Oxymoron?* 78 NEB. L. REV. 386 (1999).

[20] Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996). The employer promised that "all e-mail communications would remain confidential and privileged" and that "e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand." Id. at 98.

1. The ECPA and E-Mail Monitoring in the Workplace

In general, Title I of the ECPA prohibits: (1) intentional interceptions of transitory electronic communications, and (2) intentional uses or disclosures of content procured by interceptions of transitory electronic communications.[21] There are two important exceptions to ECPA's prohibition on intentional interceptions: (1) the "business use exception," and (2) the "consent exception."

The business use exception permits intentional and unauthorized interceptions if the interceptions are "within the regular course of business" and if the employer has a "legal interest" in the subject matter of the communication.[22] Although an employer may monitor business communications, the scope of the exception does not include personal communications. For example, and by analogy, one court has held that when an employee uses an employer's phone to conduct a job interview with a potentially new employer, such a conversation may not be monitored because it is not within the regular course of business.[23] On the other hand, a court has found a telephone call to be within the regular course of business: (1) when the call was between employees; (2) when the call was made during office hours; and (3) when the remarks were about a supervisor.[24] Similarly, it has been held that an employer may monitor an employee's phone conversation when the employer suspects that the employee is revealing confidential trade secrets and the monitoring is limited in time and purpose.[25]

If an employer would like to possess the legal ability to continually monitor all electronic communications, it is advisable for the employer to articulate such a policy in writing and define the exact nature and scope of the monitoring process. Again, by analogy, one court has held that a policy of monitoring all telephone calls constitutes a monitoring within the ordinary course of business, provided that all employees were aware that the phones would be monitored for "quality control."[26] As such, all written policies should be distributed to all employees.

---

[21] 18 U.S.C. § 2511(1).

[22] See 18 U.S.C. § 2510(5)(a)(1).

[23] Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

[24] Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986).

[25] Briggs v. Am. Air Filter Co., 630 F.2d 414 (5th Cir. 1980).

[26] Simmons v. Southwestern Bell Telephone Co., 452 F. Supp. 392 (W.D. Okla. 1978).

The consent exception permits intentional interceptions when there has been express or implied consent.[27] This exception requires that an employer give notice of monitoring to employees in order to avoid liability. One court held that notice need not be formal, but it should be "more than casual" and should communicate the full scope of the monitoring.[28] Another court has held that notice by itself is not enough and that assent may be required.[29] Finally, it is important to note that the element of consent is satisfied even if only one party to the communication has consented.[30]

Title II of the ECPA provides for civil and criminal liability for the intentional and unauthorized access to stored electronic communications.[31] Even if an employer does not have the right to "intercept" an electronic message, the employer may still be able to access the message once it is in electronic storage. However, the extent to which an employer may be able to monitor stored employee communications under the ECPA will depend largely on the judicial interpretation of the term, "authorized." For example, a court may or may not find that employee authorization is implicit since the employee is obviously aware that the communications are being stored on the employer's own computer.

When reading Title I and Title II of ECPA together, the question arises: Does an unopened e-mail constitute a transitory communication or a stored communication? The difference is significant, because statutory damages for stored communications are $1,000 per violation, while statutory damages for intercepting transitory communications are $10,000 per violation. One federal court has held that an unopened e-mail constitutes a stored communication for the purposes of the ECPA, and that the intentional and unauthorized access to an unopened e-mail may lead to liability equivalent to $1,000 per violation.[32]

Employers need to be cognizant that their voice-mail systems may be covered by the ECPA. Many voice-mail systems today store telephone phone messages electronically on a computer server. Thus, the ECPA would prohibit accessing (listening) of these telephone messages unless the employer's activities falls within the ECPA's exceptions.

---

[27] See U.S. v. Lanoue, 71 F.3d 966 (1st Cir. 1995).

[28] See Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993).

[29] See Deal v. Spears, 980 F.2d 1153. (8th Cir. 1992).

[30] See 18 U.S.C. § 2511(2)(d).

[31] 18 U.S.C. § 2701(a).

[32] See Steve Jackson Games v. U.S. Secret Service, 816 F. Supp. 432, 460 n.5 (W.D. Tex. 1993).

2. The Reasonable Expectation of Privacy and Employee Computers: The Constitutional Dimension

In assessing an employee's expectation of privacy in the workplace, it is important to distinguish between government employers and private employers. The distinction is important because in order to trigger the Fourth Amendment the search or seizure must be by a government or state actor. Private employers are not bound by the constraints of the Fourth Amendment unless their actions were at the behest of government officials. Given this important distinction, an initial examination regarding areas of Fourth Amendment jurisprudence that apply to both the government workplace and the private workplace is necessary. Only then can the unique government workplace settings be addressed.

a. The Government Workplace and the Private Workplace: Common Threads

A number of initial hurdles must be cleared in asserting a reasonable expectation of privacy in data stored on an employee's work computer. These initial hurdles deal with the numerous exceptions courts have carved out of the sweeping language of the Fourth Amendment. Although there are numerous exceptions to the Fourth Amendment, the plain view doctrine and consent are particularly relevant in the area of employee computers.

i. The Plain View Doctrine

The plain view doctrine permits seizure of evidence without a warrant if an officer is "in a lawful position to observe the evidence, and its incriminating" nature is immediately apparent.[33] Justice Harlan, in his *Katz* concurrence, succinctly expressed the rationale behind the plain view doctrine stating, "objects, activities or statements that [one] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to [one]self has been exhibited."[34] In the computer context, e-mail or other electronic messaging that require no password for access and are open to all employees, as well as personal data stored on a work computer, may be subject to the plain view doctrine.[35] The plain view doctrine arguably would likely apply in these

---

[33] See generally Horton v. California, 496 U.S. 128, 133 (1990) (stating if evidence is in plain view, then observing it or seizing it would not infringe on the right of privacy).

[34] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[35] See Bohach v. City of Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996); see also Scott A. Sundstrom, *You've Got Mail! (and the Government Knows It): Applying the Fourth Amendment to Workplace E-mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2085 (1998) (citing Bohach v. City of Reno, 932 F. Supp. at 1234-35 in support of a similar proposition involving privacy and paging systems).

circumstances because no reasonable expectation of privacy could be asserted when such a large number of employees would have access to the messages sent. In practical terms, however, this particular situation is fairly rare because most workplaces provide their employees with individual passwords in order to ensure some semblance of privacy in e-mail transmissions. Password-based access restriction would take e-mail and other electronic communications out of the purview of the plain view doctrine, as third-party access to the transmitted material would be practically nonexistent.

The other specific factual situation where the plain view doctrine might apply is through a process of timesharing in which multiple users share concurrently the resources of a single computer system. Examples of timesharing include the commercial sale of computer time, provision of computer resources to faculty and students by a university, and provision of such resources to employees by a business organization. Like e-mail messaging where the use of the timeshared computer or network is not apportioned off by the use of passwords, the computer data is arguably to the plain view doctrine. This might be the case true if the data is saved to a communal hard drive networked throughout the business or organization. For example, it is the practice at some law reviews which are linked to the university network to save all law review material to a networked hard drive that is dedicated to law review use. All members of the law review can access this networked hard drive and save personal or law review related material to this drive. Even though a password is required to initially access the particular computer station, the material saved to that networked drive is essentially shared by all law review staff. Thus, a law review member who was saving child pornography to this networked drive would have no reasonable expectation of privacy in those images given the large number of people that have access to that drive.

Therefore, in the majority of government workplace situations the employee may safely store data on a work computer without fear the plain view doctrine will strip him of his constitutional rights under the Fourth Amendment.[36] Employees should, however, inquire as to: (1) the individual password restrictions instituted by the company or government agency; (2) the appropriate place to save and store data to limit access; and (3) the number of employees that have unrestricted access to all employee computers regardless of password protections.[37]

---

[36] See 1 WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, CRIMINAL PROCEDURE § 2.6(f)(1999) (stating that users of multi-user systems still maintain an expectation of privacy despite the fact that those who operate the system may need to access that user's information in order to appropriately bill the user and to make occasional back-ups of the information to protect against accidental data loss).

[37] See generally Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 83 (1994).

ii. The Consent Exception

The consent exception to the Fourth Amendment is implicated more deeply in the workplace than in the limited factual situations discussed above concerning plain view. The consent of "one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom the authority is shared."[38] Thus, if several people own or use a particular computer, any one of those people could consent to search the "common area" of the computer. The scope of consent is also limited to the type of evidence involved in the suspected offense. In *United States v. Turner*,[39] the court ruled that officers exceeded the scope of the defendant's consent by searching the hard drive of his personal computer while investigating an assault. The court stated that an objectively reasonable person assessing the exchange between the defendant and the detectives would have understood that the police intended to search only in places where an intruder hastily might have disposed of any physical evidence of an assault. The court continued by finding the officers were limited to searching those plausible areas where physical evidence of an assault could be located, and that a computer hard drive clearly was not one of those areas.

The area of greatest ferment in the consent area deals with workplace policies governing Internet use and the monitoring of e-mail transmissions. Accepting or continuing employment with a company or governmental agency which has instituted such a policy may operate as employee consent and could bar application of Fourth Amendment protections. In *United States v. Simons*,[40] defendant Simons was employed with the Foreign Bureau of Information Services (FBIS), a division of the Central Intelligence Agency (CIA), as an electronic engineer. The Systems Operation Center Manager, who manages the computer network for FBIS, was investigating the capabilities of a new system placed on the FBIS network that logged all computer traffic going outside the network. A component of this program allowed the systems manager to do a keyword search of the logged material. The systems manager, attempting to discover if the new program could unearth inappropriate Internet usage, ran the keyword "sex." A significant number of responses were traced back to a particular workstation, later determined to

---

[38] United States v. Matlock, 415 U.S. 164, 170 (1974). The Court further noted "common authority" is not defined by traditional notions of property law, but: rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their numbers might permit the common area to be searched. Id. at 171 n.7.

[39] United States v. Turner, 169 F.3d 84, 87 (1st Cir. 1999).

[40] United States v. Simons, 29 F. Supp. 2d 324, 327 (E.D. Va. 1998), *aff'd*, 2000 WL 223332 (4th Cir. 2000).

belong to the defendant. The search results indicated that the accessed Internet sites appeared to be pornographic in nature, and the frequency with which these sites were accessed eliminated any possibility of accidental activity. Upon direction of his supervisor, the systems manager verified the sites were pornographic, accessed defendant's computer through the network, and discovered over 1,000 downloaded graphic files containing pornographic material. The systems manager copied defendant's hard drive via the network. This copy was then handed over to the special investigation unit of the CIA where it was discovered that a number of the downloaded graphic files depicted child pornography. A special agent obtained a search warrant permitting the agent to copy defendant's hard drive, floppy disks, documents concerning screen names, and personal correspondence.

Simons claimed the searches were conducted in violation of the Fourth Amendment and, therefore, all evidence should be suppressed. In affirming the district court's denial of defendant's motion to suppress, the Fourth Circuit relied heavily on the FBIS's official policy regarding computer use:

> Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy. The policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use.[41]

---

[41] 2000 WL 223332, at 4. The applicable section of the FBIS policy provided:

> Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall . . . be capable of recording:
>
> -- Access to the system, including successful and failed login attempts, and logouts;
>
> -- Inbound and Outbound file transfers;
>
> -- Sent and received e-mail messages;
>
> -- Web sites visited, including uniform resource locator (URL) of pages retrieved;
>
> -- Date, Time, and user associated with each event.

In light of this specific policy, the court ruled defendant had no reasonable expectation of privacy regarding his Internet usage. The court gave significant weight to the portion of the policy stating that audits shall be implemented to support identification, termination, and prosecution of unauthorized activity. The court also gave weight to the part of the policy providing that audits would be capable of recording web sites visited.

Balancing the Fourth Amendment's protections of government employees against unreasonable searches by government employers against the interests in workplace efficiency, the Supreme Court has carved out Fourth Amendment exception designed to safeguard the government's ability to properly and effectively supervise, control, and run the government workplace.[42] In *O'Connor v. Ortega*, the Court ruled that workplace searches are exempt from the Fourth Amendment in the case of an investigation into work-related employee misfeasance.

Although in theory government employees enjoy greater protections against workplace searches and seizures of their computers than their private-sector counterparts, in view of the workplace exception carved out in *O'Connor*, these additional protections arguably are limited.

B. Data Collection

A survey released by the Electronic Privacy Information Center found that nearly half of the 100 most popular Web sites collected information from users.[43] Personal information about Internet users is becoming easy to collect, or some may even say steal, due to software implementations known as "cookies" mentioned earlier.

1. Federal Legislation Regulating Internet Service Providers: The ECPA

Statutory protection of personal information in the United States generally targets specific, sectoral activities, such as video rentals under the Video Privacy Protection Act.[44] But even the Video Privacy Protection Act does not prohibit disclosure of video content chosen from a Web site.

The Electronics Communications Privacy Act ("ECPA") is the statute most likely to

---

[42] O'Connor v. Ortega, 480 U.S. 709 (1987).

[43] See Electronic Privacy Information Center, *Surfer Beware: Personal Privacy and the Internet,* at <http://www.epic.org/reports/surfer-beware.html>.

[44] 18 U.S.C. § 2710.

provide restrictions on an ISP's data use.[45] The ECPA is currently the most comprehensive data protection legislation that protects personal information on the Internet. The Act covers all forms of digital communication, including transmissions of text and digitized images, in addition to voice communication.[46] It prohibits unauthorized eavesdropping not only by the government, but by all persons and businesses.[47] The ECPA forbids unauthorized access to an electronic communication while in storage in an electronic communication service facility.[48] The Act protects "wire, oral, or electronic communications" against warrantless interception by law enforcement officers, and criminalizes such interception by other persons.[49] The ECPA also prohibits unauthorized access to messages stored on computer systems, and unauthorized interception of messages in transmission.[50]

The ECPA may not prohibit disclosure of personal information to the private sector, but section 2703 does strictly limit the information that electronic communications providers and ISPs may give to the government. Pursuant to sections 2703(a) and (b), in order for a government entity to obtain user information, it must first obtain a subpoena, warrant, or court order. If the government seeks the contents of a communication rather than the records pertaining to a user, more stringent procedural safeguards apply. For communications that have been in electronic storage for 180 days or fewer, the government must obtain a warrant from the U.S. Attorney.[51] General or an equivalent state warrant. If the communication has been stored for more than 180 days, the government must obtain either a warrant, subpoena, or court order and give the user notice before the contents are released.[52] System operators who cooperate with government agents that have proper warrants and court orders are not held subject to legal action by users whose messages are seized by the government.[53]

---

[45] 18 U.S.C. §§ 2510-2522, 2701-2709, 3121-3126.

[46] See id. §§ 2510-2521.

[47] See id. § 2510.

[48] See 18 U.S.C. § 2701(a).

[49] 18 U.S.C.A. §§ 2511, 2517(4), 2516.

[50] See id. § 2511.

[51] See id. §§ 2510-2521.

[52] See id. §§ 2510-2522; 2701-2709; 3121-3126.

[53] See id. § 2703.

Subsections (a) and (b) clearly apply to the conduct of the government. Two courts have directly contradicted each other in determinations regarding subsection (c), which lists the only instances in which an electronic communications service provider may disclose subscriber information (exclusive of content) to a government entity. Those two cases are discussed below.

The ECPA contains numerous exceptions. The ECPA does not assure on-line system users' privacy rights from system operators for stored messages.[54] Since a system can be configured to store all messages that pass through it, the operator effectively has the ability to review all messages that pass through the system. Under the ECPA, it is illegal for a system operator to reveal stored private messages or users to anyone else.[55] It is legal, however, to reveal messages falling under certain specific exceptions noted in the ECPA.[56] For instance, a message sent to the operator himself can be disclosed, if he so chooses, since the operator is treated like any other recipient of a letter.

Another exception involves divulging information to government authorities. A message that is accidentally obtained by a system operator can be disclosed to legal authorities if the operator believes that illegal activity is taking place over the system.[57] Authorities then have the right to review these messages to the extent they deem necessary to confirm the system operator's apprehensions.[58] If, however, the authorities want to intercept or review messages at their leisure, they must first obtain an appropriate warrant from a judge or magistrate.

If the system operator happens to violate a user's privacy rights under the ECPA, such as posting private e-mail to the public, the ECPA gives the user the right to sue the system operator.[59] The system operator must then remove the public posting and can be held responsible for any monetary damages incurred as a result of the privacy violation.[60] The ECPA also allows

---

[54] See id. § 2702(b).

[55] See id.

[56] See id.

[57] See id. § 2702(b)(6).

[58] See id. § 2703.

[59] See id. §§ 2520, 2707.

[60] See id.

for recovery of attorney fees.[61] This is especially important in cases where proving operator misconduct or determining the dollar amount of damage is so difficult that users would otherwise refrain from bringing the case to court in the face of high legal costs. There are also criminal penalties for violating the ECPA.[62]

Some commentators have argued that because the ECPA's protection for electronic mail is similar to that for telephone calls, the two should be treated similarly for privilege purposes. For instance, system administrators of an "electronic services provider," like telephone company employees, may intercept communications when necessary for provision of service or to protect their property, pursuant to 18 U.S.C. § 2511(2)(a)(i). However, it is unclear whether the ECPA's "electronic services provider" provisions apply to Internet transmission. Cases such as *State Wide Photocopy Corp. v. Tokai Financial Services, Inc.*,[63] have found the ECPA's electronic services provider provisions available only to entities that actually provide services to the public. The limitations contained in ISP contracts and interconnection agreements may preclude application of the ECPA, as may the fact that some ISPs do not provide services to the public per se, but only to corporate entities.

While the ECPA specifically forbids providers from divulging the contents of electronic communications during transmission or storage, this protection is limited, as one commentator has noted:

> Although this may seem to bar communication providers from peddling personal information in the marketplace, such privacy protections are illusory. The . . . bar applies solely to the contents of communications, not to transactional records, that may be freely disclosed to anyone other than a governmental entity. Unfortunately, the line is not bright between the contents of a communication and the transactional data about that communication. . . . The legislative history adds little light, except to make clear that "contents" do not include "the identity of the parties or the existence of the communication."[64]

---

[61] See id. §§ 2520(b)(3), 2707(b)(3).

[62] See id. § 2701(b).

[63] 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (application of ECPA denied because party does not "provide[ ] a communication service to the public, but ... is in the business of financing and ... merely uses fax machines and computers as necessary tools of almost any business today").

[64] Kang, *supra* note 9, at 1234-35.

a. ISP Disclosure of Personal Information to a Third-Party

The ECPA's provision on "unauthorized access" does not include access to personal data authorized by an ISP.[65] Thus, an ISP's sale of its customers' personal data is not "unauthorized access" under the ECPA. Moreover, the ECPA's protection for subscriber records only limits release to "a governmental entity."[66] ISPs are free to sell and share these data to anyone other than the government.

i. McVeigh v. Cohen, 983 F. Supp 215 (D.D.C. 1998).

A 1998 federal case, *McVeigh v. Cohen*,[67] illustrates the ISP's key role in Internet privacy. *McVeigh* demonstrates how ISPs can link information about a person's identity offline to information about their behavior online.

In 1996, America Online (AOL) surrendered subscriber information about Timothy McVeigh -- a Navy serviceman, an AOL customer, but not *the* Timothy McVeigh of Oklahoma City infamy -- to the United States Navy. An investigation was initiated after McVeigh sent an e-mail to a crew member's wife, who was a volunteer for a charity. AOL provides its subscribers with up to five different e-mail names. McVeigh used his AOL account to join in a charity drive, but inadvertently sent his communication under his e-mail name "boysrch."

Through an option available to AOL subscribers, the crew member's wife searched through the "member profile directory" to locate additional information about the sender of the e-mail. Although this profile did not include his full name, address, or phone number, it specified that "boysrch" was an AOL subscriber named Tim who lived in Honolulu, worked in the military, and identified his marital status as "gay." After McVeigh's e-mail and directory information were brought to the Navy's attention, a military investigator promptly contacted AOL. Without identifying himself as representing the government, the investigator explained that he wished to find out the identity of "boysrch." Despite its established privacy policy to the contrary, AOL turned over the subscriber data linking McVeigh to the specific account. AOL has in the past sold subscriber information to third parties, such as direct marketers. It even proposed to sell home phone numbers before a storm of protest forced it to change this plan.[68]

---

[65] 18 U.S.C. § 2701(c)(1).

[66] 18 U.S.C. § 2703(c)(1). See Tucker v. Waddell, 83 F.3d 688, 691 (4th Cir. 1996) (noting ECPA's private cause of action against governmental entities that violate it).

[67] 983 F. Supp 215 (D.D.C. 1998).

[68] See Seth Schiesel, *American Online Backs Off Plan to Give Out Phone Numbers*, N.Y. Times On the Web 1-3 (July 25, 1997) <http://

In *McVeigh*, Judge Sporkin held that the government's behavior violated its "Don't Ask, Don't Tell" policy regarding gay armed forces personnel. The violation of the policy occurred because the Navy contacted AOL without the "credible information" required to initiate such an investigation. Judge Sporkin also noted that the Navy's action had likely violated the ECPA's ban on disclosure of telecommunication subscriber data to the government without a subpoena.[69]

The ECPA provides that an ISP shall disclose information pertaining to a subscriber to a governmental entity only when the governmental entity (a) obtains a warrant or (b) gives prior notice to the subscriber and issues a subpoena or receives a court order authorizing disclosure of the information.[70] The court rejected the government's argument that Section 2703(c)(1)(B) obligates the ISP to withhold the information from the government, but does not impose any restrictions on the government itself. The court concluded that such provision must be read in the context of the statute as a whole, and that all provisions of Section 2703 were intended to work in tandem -- with respect to both the ISP and the government -- to protect consumer privacy. (Such a conclusion is directly contradicted by the Fourth Circuit's holding in *Tucker v. Waddell*[71] that Section 2073(c) only prohibits actions of ISPs.)

The court further concluded that even if the government's interpretation of Section 2703(c)(1)(B) were correct, there was a likelihood of success on the merits with respect to plaintiff's claims under Section 2703(a) and (b) -- which set out the circumstances in which a governmental entity may require disclosure of electronic communications -- that the government solicited violation of the ECPA by AOL.

The court's analysis may have been influenced in part by Judge Sporkin's apparent views of the injustice committed by the Navy in seeking out evidence of Mr. McVeigh's homosexuality when he did nothing to compromise the "Don't Ask, Don't Tell" policy. According to the court, "suggestions of sexual orientation in a private, anonymous e-mail" did not give the Navy sufficient reason to investigate.

The *McVeigh* case reveals how little protection exists for most Americans whose personal data are found in cyberspace. If McVeigh had worked for a private company rather than the Navy, Judge Sporkin's hands would have been tied. McVeigh received additional privacy

---

www.nytimes.com/library/cyber/week/-072597aol.htm>; Evan Hendricks, *American Online Snoops Into Subscribers' Incomes, Children*, Privacy Times, Dec. 15, 1997, at 1-3.

[69] McVeigh v. Cohen, 983 F. Supp. 215, 219-20 (D.D.C. 1998).

[70] 18 U.S.C. § 2073(c)(1)(B).

[71] 83 F.3d 688 (4th Cir. 1996).

protection from the "Don't Ask, Don't Tell" policy. Moreover, the ECPA would not have prevented AOL from releasing McVeigh's personal subscriber data to a private employer. The ECPA generally permits ISPs to disclose subscriber information to entities other than the government. Indeed, since the Navy investigator had represented himself as a private, nongovernmental person, AOL had a strong argument that it had not violated the ECPA.[72]

ii. Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996)

The Fourth Circuit held that Section 2703(c)(1)(B) of the ECPA only prohibits actions of ISPs and not those of the government. In that case police officers in Durham, North Carolina obtained subscriber information from GTE South through use of improper subpoenas. In interpreting § 2703(c), the court noted that the ECPA was modeled on the Right to Financial Privacy Act, which, unlike the ECPA, contains, in addition to provisions limiting circumstances under which records may be disclosed to the government, a "companion" section limiting circumstances under which the government may obtain access to customer records. The court noted in dicta that "it might be possible for a governmental entity to violate § 2703(c) by aiding and abetting or conspiring in the provider's violation," although such claims were not alleged in the case.[73]

2. Federal Legislation Regulating Web sites: The Child Online Privacy Protection Act

In its congressional reports, the FTC declined to recommend generally-applicable privacy legislation. The Commission did, however, recommend in the 1998 report that Congress adopt legislation to protect children online. The March 1998 survey of Web sites had identified 212 sites (from a sample of 1,402) directed at children. Eighty-nine percent of them collected children's personal information, but few allowed for meaningful parental involvement. The Commission was concerned that section 5 of the FTC Act might not reach all questionable practices, including the collection of personal information from children. In particular, section 5 would not necessarily authorize the Commission to require parental notice and involvement across the board for all commercial Web sites engaged in collecting information from children. Therefore, the Commission recommended that Congress take action; four months later, the president signed the Child Online Privacy Protection Act of 1998.

---

[72] See *AOL Admits Error in Gay Sailor* Case, N.Y. Times on the Web 1 (Jan. 21, 1998) <http://www.nytimes.com/aponline/w/AP-Navy-Gay- Dismissal.html>; [FN179]. See Carl S. Kaplan, *Sailor's Case Leaves Question of Liability*, N.Y. Times on the Web 2-3 <http://www.nytimes.com/library/cyber/law/012998law.html>.

[73] See also United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999)(ECPA concern for privacy extends only to government invasions of privacy; ISPs are free to turn stored data and transactional records over to nongovernmental entities).

The Child Online Privacy Protection Act of 1998 (COPPA) was enacted in response to the Supreme Court's 1997 decision in *Reno v. ACLU*,[74] invalidating the obscenity provisions of the Communications Decency Act (CDA).[75] The House Commerce Committee Report stated that the COPPA "has been carefully drafted to respond to the Supreme Court's decision in [first ACLU case]."[76] The COPPA requires Web sites directed to children to follow fair information standards. This law also explicitly grants the FTC power to develop privacy standards for Web sites directed at children and to investigate violations of these standards as an unfair or deceptive act or practice.[77]

The COPPA prohibits "knowingly and with knowledge of the character of the material . . . by means of the World Wide Web, mak[ing] any communication for commercial purposes . . . available to any minor . . . that includes any material that is harmful to minors . . . ."[78] The COPPA is narrower than the CDA in several respects. First, the COPPA only applies to Web communications. Second, only communications for commercial purposes are affected. Third, unlike the "indecent and patently offensive" standards in the CDA, the COPPA applies to communications that are "harmful to minors."

Noncompliance with the COPPA carries criminal and civil penalties, including fines and imprisonment.[79] The Act establishes safe harbors for compliance with a set of self-regulatory

---

[74] 521 U.S. 844, 868-73 (1997).

[75] In *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999), the district court issued a preliminary injunction enjoining enforcement of the obscenity provisions of COPPA.

[76] H.R. Rep. No. 105-775, at 5 (1998).

[77] See Dorothy A. Hertzel, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L.J. 429 (2000).

[78] 47 U.S.C.A. § 231(a)(1).

[79] The COPPA provides:

> (a) Requirement to restrict access. (1) Prohibited conduct. Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.
>
> (b) (2) Intentional violations. In addition to the penalties under paragraph (1), whoever intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. For purposes of this paragraph, each day of

guidelines issued by representatives of the marketing or online industries. The FTC is directed to provide incentives for industry self regulation and respond to requests for safe harbors. Like the CDA, the COPPA provides affirmative good faith defenses, including "requiring use of a credit card, debit account, adult access code, or adult personal identification number; . . . accepting a digital certificate that verifies age; or . . . other reasonable measures that are feasible under available technology."[80]

COPPA requires the FTC to adopt regulations for commercial Web sites regarding the collection, use, and disclosure of information about children under the age of thirteen. In April 2000, the FTC issued rules to implement COPPA.[81] The FTC rules requires the operator of any Web site or online service directed to children (under 13 years of age) that collects personal information from children to

- provide notice of its information practices;
- obtain verifiable parental consent, subject to certain limited exceptions;
- provide parental access to collected information and an opportunity to refuse further use of collected information;
- prohibit conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary; and
- require operators to establish or maintain security procedures.[82]

The rules directly affect those franchisors whose Web sites include pages geared toward children, such as the "kids club" pages of many fast-food chains. In fact, the rules apply to every

---

violation shall constitute a separate violation.

(3) Civil Penalty. In addition to the penalties under paragraphs (1) and (2), whoever violates paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

[80] Id. § 231(c)(1).

[81] See 16 C.F.R. § 312.1 (2000).

[82] See id. § 312.3.

Web site that is either targeted to children under the age of thirteen or whose owner has actual knowledge that the site is visited by children under thirteen. The rules govern notices Web sites must give about information practices, how Web sites treat personal information obtained from children under thirteen, and what rights parents have with respect to such information.

The FTC's rules also require parental consent for most uses of a child's personal information.[83] The question of how to obtain verifiable parental consent is one of the most controversial raised in the FTC rulemaking. Most companies that submitted comments in the rulemaking did not want the FTC to prescribe specific technology or to limit the ways that companies can obtain verifiable parental consent. The FTC's challenge was to find a method that neither imposes an excessive burden nor encourages children to provide false information to sign on to restricted Web sites. The FTC's COPPA regulations provide the following methods for verifying parental consent:

> Methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph. Provided that: For the period until April 21, 2002, methods to obtain verifiable parental consent for uses of information other than the "disclosures" defined by § 312.2 may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Operators who use such methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.[84]

Recognizing the value and flexibility of industry self-regulation, the FTC adopted a "safe harbor" for self-regulatory programs that the Commission certifies as equally protective of children's

---

[83] See id. § 312.5.

[84] 16 C.F.R. § 312.5(b)(2).

privacy.[85] The safe harbor enables franchisors to comply with COPPA by joining children's programs such as those sponsored by TRUSTe and BBBOnLine.

3. FTC Enforcement Activity

FTC encouragement of self-regulation has not precluded use of the agency's enforcement powers against online data collectors. The FTC reportedly has more than eighty investigations under way concerning cyberspace matters. Two enforcement actions involving children's online privacy already have been settled.

a. GeoCities Complaint

The FTC's enforcement action against the GeoCities company highlights the leaky privacy protection offered at Web sites.[86] GeoCities markets itself as a "virtual community" that organizes its members' home pages into forty different areas, termed "neighborhoods." In these areas, members can post a personal Web page, receive e-mail, and participate in chat rooms. Non-members can also visit many areas of GeoCities.

According to the FTC, GeoCities engaged in two kinds of deceptive practices in connection with its collection and use of personal information. First, although GeoCities promised a limited use of the data it collected, it in fact sold, rented, and otherwise disclosed this information to third parties who used it for purposes well beyond the scope of permission given by individuals. Second, GeoCities promised that it would be responsible for maintenance of the data collected from children

---

[85] 16 C.F.R. § 312.10 provides:

> Safe harbors.
>
> (a) In general. An operator will be deemed to be in compliance with the requirements of this part if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission.

[86] See GeoCities, File No. 9823015 (Fed. Trade Comm. 1998) (agreement containing consent order). The GeoCities Consent Order can also be found at < http://www.ftc.gov/os/1998/-9808/geo-ord.htm>. For a discussion, see FTC, Analysis of Proposed Consent Order to Aid Public Comment <http:www.ftc.gov/os/1998/9808/9823015.- ana.htm>. The GeoCities Web site is located at <http://www.geocities.com>.

in the "Enchanted Forest" part of its Web site. Instead, it turned such personal information over to third parties called "community leaders."

GeoCities settled with the FTC and promised to make significant changes in its privacy practices.[87] The final order permits GeoCities to collect or use personal data about children to the extent permitted by the Children's Online Privacy Protection Act of 1998. The settlement is generally regarded as a model for ISP self-regulation policies.[88] In the absence of self-regulation or new legislation, the case also brings into question the extent to which ISPs will seek to shield themselves from liability for deceptive practices by not establishing a privacy policy in the first instance.

b. Liberty Financial Services Complaint

In May 1999, the FTC issued a complaint and proposed consent order arising from its investigation of the Liberty Financial Services (LFS) Web site. The LFS Web site features several areas targeted to children and teens, surveying them about weekly allowances; types of financial gifts received, such as stocks, bonds, and mutual funds, and the source of such gifts; spending habits; part-time work history; college plans; and family finances. The survey also collects the individual's name, address, age, and e- mail address.

The FTC alleged that LFS made three misrepresentations concerning its information practices. First, LFS represented that information collected on its Web site would be totally "anonymous," when it was in fact collected and maintained in a database that allowed individual identification. Second, according to the FTC, individuals who completed the survey were promised they would receive the company's Young Investor e-mail newsletter; in fact, no such newsletters were ever provided. Third, LFS falsely represented that, every three months, a participant in the survey would be selected to win specified prizes. According to the complaint, LFS did not select any winners as represented.

The proposed consent order prohibits LFS from misrepresenting its use and collection of

---

[87] See GeoCities Proposed Consent Agreement, 63 Fed. Reg. 44,624 (1998) (final approval Feb. 12, 1999); FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case <http://www.ftc.gov/-opa/1998/9808/geocitie.htm>; Saul Hansell, Amid Downturn, Another Internet Company's IPO Catches Fire N.Y. Times on the Web (Aug. 12, 1998) <http:www.nytimes.com/library/tech/98/- 08/biztech/articles/12geocities-ipo.html>.

[88] See JEFFREY P. CUNARD, JENNIFER B. COPLAN & GEORGE VRADENBURG, III, COMMUNICATIONS LAW 1999, 581 PLI/PAT 853 (Nov. 1999).

personal information and requires parental consent to provide the information.[89] LFS must post a clearly articulated privacy policy that clarifies what information is collected, how it is used, and how the consumer can access his personal data. LFS must post this notice at every area on the site where personal data are collected, accompanied by the following statement: "Notice: We collect personal information on this site: To learn more about how we use your information, click here." Finally, the order requires LFS to delete information previously collected from children and to implement specific procedures to obtain "verifiable parental consent" prior to collecting and using children's data.

The GeoCities and LFS enforcement actions applied traditional FTC deception law. The FTC did not allege that collecting or using information, by itself, violated the FTC Act; rather, the FTC alleged that the information practices violated the law because they were different from the practices that had been represented to Web site users. Similar behavior elsewhere on the Web is unaffected by this FTC enforcement action, with the possible exception of behavior affecting children since passage of the Children's Online Protection Act of 1998. Indeed, the FTC's ability to engage in these kinds of investigations is itself limited. The FTC was able to obtain jurisdiction in this case only because GeoCities' false representations regarding its privacy practices constituted "deceptive acts or practices" within the meaning of under the Federal Trade Commission Act. Web sites which give no assurances about privacy, therefore, are not only unaffected by the GeoCities consent order, but also are likely to fall outside the FTC's jurisdiction. But the terms of the consent orders suggest that the FTC may be moving toward a view that failure to follow its fair information practices is inherently deceptive or unfair. Because the consent orders are as much regulatory as remedial in nature, they also serve as a preview of what privacy legislation might require if enacted.

Another statutory limit exists on the FTC's jurisdiction. The FTC's enabling act restricts its powers to situations where an unfair act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[90] As this statutory language indicates, the FTC may be open to challenges to its power to stop activities that it claims to be unfair or deceptive trade practices.[91]

---

[89] Liberty Fin. Serv. Co., 64 Fed. Reg. 29,031 (1999) (proposed May 28, 1999).

[90] 15 U.S.C. § 45(n). For an interpretation of the circumstances under which "substantial injury" to consumers has been found under the FTC statute, see Thompson Med. Co. v. FTC, 791 F.2d 189, 196 (D.C. Cir. 1986); International Harvester Co., 104 F.T.C. 949, 1041 (1984); PETER C. WARD, FEDERAL TRADE COMMISSION: LAW, PRACTICE AND PROCEDURE § 5.04(2) (1999).

[91] See Robert Gellman, What Policy Does FTC Set In Its GeoCities Decision?, DM News, Sept. 21, 1998, at 15. For a claim of broad enforcement authority over commerce on the Internet by the Chairman of the FTC, see FTC, Consumer Privacy on the World Wide

C. Personalization

Many companies are turning to the Internet in search of ways to get closer to their customers. In order to achieve this goal, these companies are engaging in a process known as personalization. Personalization technology generates personalized web pages for customers based on the demographic data obtained from these individuals. In addition to the information that the individuals voluntarily provide, companies also acquire demographic data by monitoring browsing and buying patterns of the individuals who visit the companies' Web sites.

The use of personalization technology is becoming common for many companies. For example, American Airlines and its cross-marketing partners, Hertz and Hilton, use personalization to improve their businesses by appealing to the needs and interests of each specific customer.[92] After accumulating information about a particular individual, a new, personalized Web page is created for that individual each time the individual enters the American Airlines Web site. A person who requests a price quote for an American Airlines flight to Boston will also receive extra information on the same web page as the ticket price, such as for a Hertz car and a Hilton hotel room during that same period. Brokerage firms also plan to use personalization technology. These firms can monitor clients' viewing preferences on the brokerage's Web site, such as their assessment of specific stock quotes, thereby allowing brokers to recommend investments related to specific stocks.

D. Anonymity

The issue of anonymity on the Internet raises heated debates between supporters of free expression and those who believe that anonymity is only a shield for people who engage in abusive, hurtful, or illegal activity. There are several explanations for why people want to hide their true identities when using the Internet. For example, a person might want to protect himself from what he perceives as an oppressive government, to send something 'off the record' to a journalist, to communicate with a self-help organization, or just politically incorrect viewpoints. Anonymity is seen as particularly important for people who wish to express their views on-line about sensitive or controversial issues, such as sexual abuse, affirmative action, and harassment, without fear of retribution or embarrassment. The lack of anonymity on the Internet can lead to public ridicule or censure, physical injury, loss of employment or status, and in some cases, even legal action.[93]

Web, <http://www.ftc.gov/-os/1998/9807/privac98.htm (prepared statement before the subcommittee on telecommunications trade and consumer protection)>.

[92] See Gregory Dalton, *Pressure for Better Privacy – Business Moves to Fend Off Regulation of Internet Data*, Information Week, at <http://www.techweb.com/se/directlink.cgi?IWK19980622S0040>.

[93] See Anonymity on the Internet (last modified Feb. 13, 1999) <http:// www.dis.org/ erehwon/anonymity.html>.

1. ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997)

In 1996, Georgia passed Act No. 1029 (codified at O.C.G.A. § 16-9-93.1) which makes it a crime for any person knowingly to transmit any data through a computer network

> (1) ... if such data uses any individual name ... to falsely identify the person ... or
> (2) ... if such data uses any trade name, registered trademark, logo ... which would falsely state or imply ... that such person has permission to use it.

The ACLU and others challenged the statute as imposing unconstitutional content-based restrictions on their right to communicate anonymously and pseudonymously over the Internet, and on their right to use trade names and logos in a manner otherwise held to be constitutional. Citing the Supreme Court's decision in *McIntyre v. Ohio*,[94] Judge Marvin Shoob of the Northern District of Georgia concluded that the identity of the speaker is no different from other components of a document's contents. Accordingly, the Act's prohibition of Internet transmissions which "falsely identify" the sender constitutes a presumptively invalid content-based restriction. Applying a strict standard analysis, the court agreed that fraud prevention is a compelling state interest, but held that the Act is not narrowly tailored to achieve that purpose. The court concluded that, on its face, the Act prohibits protected speech such as false identification to avoid ostracism, discrimination, harassment or to protect privacy. For similar reasons the court concluded that the plaintiffs would likely succeed on their claims that the Act is overbroad.

E. Invasion of Privacy in Non-Workplace Settings

1. Investigative Searches by Law Enforcement Agencies: The Reasonable Expectation of Privacy and the Internet

In applying the reasonable expectation of privacy standard to this relatively new form of communication, courts analogize e-mail to other forms of communication.[95] In *United States v. Maxwell*,[96] the United States Court of Appeals for the Armed Forces likened e-mail to both first

---

[94] 115 S. Ct. 1511 (1995).

[95] See generally Francis A. Gilligan & Edward J. Imwinkelreid, *Cyberspace: The Newest Challenge for Traditional Legal Doctrine*, 24 RUTGERS COMPUTER & TECH. L.J. 305, 320 (1998).

[96] See United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) (stating in dicta "[m]essages sent to the public at large in the 'chat room' . . . lose any semblance of

class mail and telephone calls. In *Maxwell*, FBI agents received several e-mails and graphic files discussing and depicting child pornography from a concerned citizen, along with the screen names of the users who sent the messages and material. Based on this information, an agent sought a search warrant permitting him to discover the true identity of the users by obtaining the master list of users and screen names from the Internet service provider. Upon discovering the true identity of those involved, agents learned that the defendant, one of the users, was in the Air Force. The Air Force Office of Special Investigations thereafter obtained a warrant to search the defendant's quarters. There, a number of graphic files depicting child pornography were found on his computer. He subsequently sought suppression of all physical evidence recovered during the various searches.

The court stated that e-mail is similar to first-class mail in that "if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause."[97] The court additionally noted that e-mail shares some qualities of telephone calls as "the maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation."[98] Relying on these parallels, the court concluded that the sender of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission. The court, however, narrowly drew its ruling by stating "once the [e-mail] is received and opened, the destiny of the letter then lies in the control of the recipient of the letter, not the sender, absent some legal privilege."

The court rejected the government's argument that once the defendant disclosed the information to the Internet service provider, he thereby forfeited all Fourth Amendment protections. Although the service provider always has ultimate access to messages stored on its servers, to use the mail and telephone analogy, "[t]he post office cannot indiscriminately intercept the letters it transmits, and neither may the telephone company routinely eavesdrop on the conversations occurring on its lines."[99] Thus, defendant was permitted to litigate the issue because he had a reasonable expectation of privacy in the e-mail messages, despite the service provider's ability to access the contents of any particular message.

In addition to sending discrete electronic communications over the Internet via e-mail, e-messages may also be broadcast in Internet chat rooms. In a public chat room, it would be

---

privacy").

[97] Id. at 417.

[98] Id. at 418.

[99] Id. at 418-19.

difficult to claim a reasonable expectation of privacy as the contents of the discussion are open for all in the chat room to read. An Ohio federal district court squarely addressed this issue in *United States v. Charbonneau.*[100]

In *Charbonneau,* an FBI agent visited various chat rooms posing as a pedophile. The agent operated primarily in private chat rooms titled "BOYS" and "PRETEEN." The agent did not actively engage in conversation with the other members of the chat room, but instead passively observed and recorded the dialog between members. Child pornography was often exchanged by using information gained during these electronic communications. The agent identified one of those involved in the distribution of the child pornography by his screen name. The agent then obtained defendant's true identity through the use of a search warrant. Defendant sought suppression of the statements he made while in the chat room as well as the e-mail messages he sent to other users.

Denying defendant's motion to suppress, the court ruled that when defendant engaged in chat room conversations, he essentially assumed the risk that one of his fellow users could possibly be a law enforcement official. The court further ruled defendant could not have a reasonable expectation of privacy because he was aware of the operating procedures in the chat room and continued to use the chat room despite its open nature.

2. Computer Searches by Persons Not Government Agents

It is, of course, basic that the Fourth Amendment is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.[101] In determining whether a private party is acting as an agent of the government, courts apply a two-pronged test. First the court must examine whether "the [g]overnment knew of or acquiesced in the intrusive conduct . . . ."[102] The court must then decide whether "the private party's purpose for conducting the search was to assist law enforcement efforts or further his own ends."[103] Searches by private parties in the computer arena normally occur when computer technicians inadvertently stumble upon illegal material when servicing a computer.

---

[100] United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).

[101] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[102] United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998).

[103] Id.

In *United States v. Hall*,[104] the defendant took the central processing unit of his computer to a local computer store for repairs. In order to diagnose the problem a computer technician accessed a number of file directories. In viewing these directories, the technician observed a number of files with sexually explicit titles. The technician opened these files and discovered what he believed to be child pornography. The technician immediately contacted local law enforcement officers who instructed him to make copies of the material. Agents eventually obtained a search warrant based solely on the technician's affidavit. The search of defendant's computer and home revealed numerous graphic images of child pornography. Defendant moved to suppress the evidence claiming an agent of the government made the discovery of the images. The Seventh Circuit affirmed the denial of defendant's motion, ruling that the technician's search was not at the behest of the government.

Similarly, in *United States v. Barth*,[105] the defendant, owner of his own accounting firm, was experiencing difficulties with his office computer and called in a computer technician to correct the problem. While searching for viruses by opening various files, the technician discovered computer images of child pornography. The technician, a confidential informant for the FBI, contacted an agent and was instructed to copy the contents of the hard drive. The following day local law enforcement agents, without a warrant, reviewed the contents of defendant's hard drive. Based solely on an affidavit detailing the technician's initial discovery, a state magistrate issued a warrant to search defendant's hard drive. A forensic computer analyst was brought in to conduct the search. Before the search began, however, the analyst was briefed about the contents of the computer and its various systemic processes. The analyst discovered further pornographic images.

In granting defendant's motion to suppress, the court found that the initial discovery by the technician constituted a search by a private party. The technician's status changed, however, when he contacted the FBI. Then, the government knew that a reliable confidential informant was in possession of a computer containing contraband. Unlike the court in *Hall*, the *Barth* court found the independent source doctrine was inapplicable.[106] Although the application for the warrant contained only information gained by the technician's initial discovery, the forensic computer analyst who conducted the search received information from the officers as to the computer's contents and operating system. Because the forensic computer analyst was aware of

---

[104] 142 F.3d 988, 993 (7th Cir. 1998).

[105] 26 F. Supp. 2d 929 (W.D. Tex. 1998).

[106] The independent source doctrine allows admission of evidence that has been discovered by means wholly independent of any constitutional violation. Nix v. Williams, 467 U.S. 431, 443 (1984).

and used the information obtained by the officers in their initial unlawful search, the analyst's search pursuant to warrant was not a 'genuinely independent source of information and evidence.

As these two cases illustrate, many computer problems can only be diagnosed and repaired by actually accessing specific files or file directories on the computer. Thus, the likelihood that inappropriate material will be discovered is substantial. Given this likelihood, it is no surprise that private computer technicians are becoming confidential informants for various law enforcement agencies. Due to the growing number of these "dual purpose" technicians and the public's reliance on these technicians for computer assistance, the legal analysis for determining when a private individual is converted into a government agent is critically important.

3. Third-Party Consent and Home Computer Systems

The in-home single system computer user, although free from the prying eyes of her employer who owns and maintains her workplace computer system, is still subject to the Fourth Amendment exception based on. third-party consent. Government officials may search premises or effects without a warrant or probable cause if a person with the proper authority has voluntarily granted consent.[107] In *United States v. Matlock* [108] the Supreme Court held that officers may obtain voluntary consent from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected. The Court explained that

> Common authority is . . . not to be implied from the mere property interest a third party has in the property. The authority which justifies the third- party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes . . . .[109]

In examining third-party consent to access to a single computer system, a third party's right to consent to the search of a home computer depends upon the steps taken to define mutually exclusive zones of privacy. In *United States v. Smith*,[110] the defendant's live-in girlfriend consented to a search of the defendant's computer located in their master bedroom. Officers accessed computer files, which were not password protected, and discovered files containing

---

[107] See Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[108] 415 U.S. 164 (1974).

[109] Id. at 171 n.7 (citations omitted).

[110] 27 F. Supp. 2d 1111 (C.D. Ill. 1998).

child pornography. At the suppression hearing, defendant's girlfriend testified that her youngest daughter would occasionally use the computer and that defendant had previously attempted to show her how to use the computer. Defendant countered that immediately prior to the search he had removed the passwords from the hardware but had kept the passwords in place on the software. The court found that defendant's girlfriend had the requisite actual authority to consent to the search of the computer. In addition to the claims of the girlfriend, the court relied heavily on the fact that officers were not hindered in their search by passwords guarding the system, thus undercutting defendant's claim he maintained exclusive and possessory control over the computer.

4. Spam

Although the collection of personal data is the major focus of privacy concerns regarding the Internet, there are other invasion of privacy issues that require revamping with regard to the Web. An example is the privacy tort of intrusion that traditionally arises when the personal space of the plaintiff is invaded either physically or visually. The typical online intrusion occurs through "spamming," the mass distribution of unsolicited and unwanted e-mail. Courts are rapidly confronting spammers and so far have consistently held in favor of plaintiffs. Congress is also examining. For example, legislation was introduced in June 1997, the Electronic Mailbox Protection Act of 1997, to protect consumers and ISPs from such unsolicited e-mails.

"Spam" is the Internet term used to describe unsolicited e-mails. It has been defined as any e-mail sent to more than 20 people the sender does not know personally. Spam is facilitated by on-line collection of personal data through Internet use. Online user information is collected and collated, and lists with certain demographics are then sold to the spammers.

Bulk e-mailers have become targets of litigation. In one case, a bulk e- mailer used a tactic known as "spoofing" to get users to read the spam they were sent. The company would allegedly make the message appear in the in-box of the users as having come from their ISP, such as Earthlink, AOL or CompuServe. Mailboxes allegedly were clogged with thousands of unwanted e-mail solicitations. The bulk e-mailer settled with the three companies for millions of dollars. The Earthlink settlement, for example, prohibits the sending of any further e-mail messages to its users for any purpose and provides for a payment of $2 million.

The Federal Trade Commission also has taken action against bulk e-mailers. One recent case in the U.S. District Court in Maryland alleges that a bulk e- mailer used commercial e-mail to promote a misleading advertising scheme.[111]

---

[111] See Kelly Hearn, *Will US crack down on rising volume of e-mail 'spam'?* CHRISTIAN SCI. MONITOR, April 17, 2000, at 13.

a. State Legislation Regulating Spam

California, Nevada, Washington, Virginia, Illinois, and Delaware have enacted legislation restricting unsolicited commercial e-mail. Many other states also are considering legislation. The extent to which state legislation in this area will stand up to Commerce Clause scrutiny after the Pataki, Engler and Johnson cases (discussed below) is uncertain. Because the sender of an e-mail message may not know, based solely on the e- mail address of the recipient, the location of the recipient, he or she will be compelled to comply with multiple -- perhaps conflicting -- state laws. Such laws arguably extend beyond their respective state borders to burden interstate commerce.

i. California: Calif. Bus. & Prof. Code §§ 17538.45 & 17538.4.

Section 17538.45 allows service providers to develop their own policies against spam and enforce those policies through the civil courts of California. 17538.4. requires unsolicited e-mailers conducting business in California to establish "a toll-free telephone number or valid sender operated return e-mail address that the recipient of the unsolicited documents may call or e-mail to notify the sender not to e-mail any further unsolicited documents."

ii. Nevada: Nev. Rev. Stat. §§ 41.730, 41.735.

The Nevada statute provides that if a person transmits, or causes to be transmitted, to a recipient an e-mail advertisement, that person is liable to the recipient for civil damages unless (a) that person has a preexisting business or personal relationship with the recipient; (b) the recipient has expressly consented to receive the item of e-mail from the person; or (c) the advertisement is readily identifiable as promotional or contains a statement providing that it is an advertisement, and clearly and conspicuously provides (1) the legal name, complete street address and e-mail address of the sender and (2) a notice providing that the recipient may decline to receive additional e-mail and procedures for opting out.

iii. Washington: Wash. Rev. Code § 19.190.020.

The Washington statute, as amended in May 1999, prohibits the initiation of the transmission of a commercial e-mail message from a computer located in Washington or to an e-mail address that the sender knows, or has reason to know, is held by a Washington resident that: (1) uses a third party's domain name without permission or otherwise misrepresents or obscures any information in identifying the point of origin or transmission path of a commercial e-mail message or (2) contains false or misleading information in the subject line.

iv. Illinois: Illinois Electronic Mail Act, Pub. Act 91-0233 (July 22, 1999).

The Illinois law bars individuals and businesses from sending unsolicited commercial e-mail to an Illinois resident when a third party's domain name is used without permission, when the point of origin or transmission path of the message is misrepresented, or when misleading or false information is contained in the subject line of the message. Illinois' law gives ISPs the right, upon the ISP's own initiative, to block the receipt or transmission of any unsolicited e-mail advertisement that it reasonably believes will violate the law.

v. Delaware: 11 Del. Code §§ 937- 938.

The Delaware law makes it a misdemeanor under Delaware law to fail to stop sending unsolicited commercial e-mail when a recipient requests to be taken off a mailing list. The Delaware law provides for jurisdiction over persons outside the state who send spam into Delaware. The law also provides that ISPs are not liable for transmitting or blocking junk mail.

vi. Virginia: Va. St. §§ 18.2-152.4, 18.2-152.12.

Virginia's law covers spam sent through any Internet service provider based in Virginia (including, e.g., AOL) and also protects such providers from being sued by computer users who receive spam. It is a misdemeanor under the law to use a false online identity to send spam, and if the spam is deemed to be malicious and results in more than $2,500 in damages to the victim, the crime is a felony punishable by up to five years in prison. The law also provides for civil penalties of $10 per message or $25,000 per day.

5. E-Mail Monitoring in Schools

School computers and school access to the Internet may function as a useful educational tool, as they are efficient sources of endless information and communications capabilities. Unfortunately, the advantages of computers and the Internet are not available risk-free. There are many dangers to be aware of when a child uses a computer, the Internet, or even an in-house e-mail system. It is well established that schools have a duty to supervise children so that students do not cause harm to themselves, to others, or to property. For this reason, and in today's political climate, a school board may choose to implement protocol which provide for the monitoring of electronic communications and documents.

A school monitoring policy may implicate the provisions of the ECPA when school officials intercept transitory student communications or when they gain unauthorized access to stored student communications. The issue of "consent" has special relevance to the ECPA's application to a public school setting. As discussed above, any claim of an ECPA violation can be defeated by a showing that the plaintiff had consented to the defendant's activities. It is unclear, however, whether the student must consent to the school's monitoring policy, whether

the student's parent or guardian may consent on behalf of the child, or whether the school itself can satisfy the consent requirement under the doctrine of in loco parentis.

In drafting a computer and Internet policy, a school board needs to account for all relevant legal issues, such as: (1) electronic privacy; (2) sexual harassment; (3) objectionable Internet content and the use of filtering software (i.e. pornography); (4) copyright infringement and plagiarism; (5) trademark infringement; (6) the intentional or accidental destruction or alteration of student data; (7) computer crimes (i.e. hacking); (8) student freedom of expression on the Internet and in e-mails; (9) online defamation; (10) the availability of personal student information over the Internet; (11) the use of the computer or the Internet to sell drugs or commit other non- electronic crimes; and (12) the use of the computer or the Internet to break school rules.

For example, a school policy should account for issues of "electronic" sexual harassment. This is because school e-mail systems provide students with an opportunity to sexually harass other students for which school districts may be held liable. Recently, the U.S. Supreme Court held that school boards may be liable for acts of sexual harassment committed by a student against a classmate if the school board has acted with "deliberate indifference" and has "exercise[d] substantial control over both the harasser and the context in which the known harassment occur[ed]."[112] Presumably, this new rule of law would apply to acts of sexual harassment committed with the aid of the school's e-mail system. A school district may attempt to avoid liability by implementing a policy that forbids the use of the computer system for harassment purposes and which prescribes in advance the appropriate disciplinary measures for those who electronically harass other students. Schools should also implement appropriate discipline upon discovering that one student is sexually harassing a classmate.

The computer and Internet policy should also provide notice of the basic rules and procedures for use of the computer and Internet by students. The policy may provide that the computer system be used primarily for educational or career related purposes. A school board should include additional guidelines if student organizations will be permitted to create and maintain their own web site.

School web sites create additional student privacy issues. School districts must decide whether the web site will be available to anyone or whether web site access will be limited by password to students, faculty and parents. School boards must also take care not to publish sensitive and personal student identification information on school web sites such as last names, addresses, phone numbers, student photographs, etc. Finally, it would be prudent for a faculty member to act as a "gate-keeper" for all content to be posted on the school's web site. This person can make sure that the privacy and other related policies are being followed (i.e. concerning discrimination, copyright infringement, defamation).

---

[112] Davis v. Monroe County Board of Educ., 526 U.S. 629, 644 (1999).

In implementing such a policy, school boards should fully disclose to students and parents the nature of the monitoring and expressly state the complete scope of the monitoring process. After doing so, the school should acquire the consent of both the student and the student's legal guardian so that the school may intercept transitory communications and access stored electronic documents without opening itself up to an unnecessary risk of liability under the ECPA. Furthermore, a student's expectation of privacy in the school computer system may be diminished by notifying students that the computer system may be used primarily for educational purposes and that the school reserves the right to monitor or access all computer data at any time. By implementing a firm policy and by providing notice to all involved parties, a school board may conduct electronic monitoring with the greatest amount of certainty that the school board will be complying with applicable law.

IV. Responses to Privacy and the Internet in Other Countries

The urge to regulate Internet privacy is even stronger in other parts of the world, where electronic commerce is less developed than in the United States. In particular, European authorities have not been willing to give self- regulation a chance. The European Union's Directive on the Protection of Personal Data came into force on October 25, 1998.[113] It restricts the information that may be gathered about individuals in EU member states and forbids the export of personal data[114] from EU member states to any third-party nations which lack "an adequate level of protection."[115] Under the Directive, Member States are required to impose minimum standards with respect to the processing of personal data on the Internet. The Directive

---

[113] Council Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 (available at <http://www.europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html>).

[114] "Personal data" are broadly defined as "any information relating to an identified or identifiable natural person," and 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." Id. at art. 2(a). The directive also relies on the concept of "data controller," defined as the "person, public authority, agency, or other body which alone or jointly determines the purposes and means of the processing of personal data."

[115] Council Directive 95/46, art. 25, 1995 O.J. (L281) 1, 31. For a discussion, see Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and Intgernational Rules in the Ratrcheting Up of U.S. Privacy Standards,* 25 YALE J. INT'L L. 1 (2000); Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 463-66 (1995).

requires that (a) personal data may be processed only with the consent of the individual; (b) individuals be informed as to the intended purposes of such processing; (c) information not be processed in a way incompatible with such purposes; (d) individuals be given access to and ability to correct personal data and right to block processing of such data; and (e) individuals have a right to judicial remedies and compensation with respect to violations of their privacy rights. In addition, certain types of data -- relating to a person's race or ethnicity, political, religious or philosophical beliefs, trade-union membership, and health or sex life -- are accorded additional protections.

EU officials have indicated that the United States does not meet their data protection standards. Importantly, Article 25 of the Directive prohibits the transfer of personal data to countries outside the EU that do not guarantee "adequate" privacy protections. Given the European perception that the United States does not fully protect personal privacy to the extent common in Europe, there is substantial concern in the U.S. that the directive amounts to a trade barrier that will substantially restrict the flow of electronic commerce. The Directive does not define the term "adequate", and provides that determinations as to adequacy will be made on a case-by-case basis, taking into account all of the surrounding circumstances. Notwithstanding the lack of comprehensive or omnibus privacy legislation in the U.S. (in contradistinction to the situation in Western Europe), many in the private and government sectors have argued that a self-regulatory regime could satisfy the directive's requirements.

In cases where adequate protection does not exist, the Directive provides exceptions that permit transfers if, among other circumstances, the individual affected has "unambiguously" consented, or if the party receiving the data has agreed by contract to provide adequate protection.[116] Whether the United States generally has "adequate" information privacy is a complex question. An answer to it requires examination of the protections available for a specific data transfer, including the safeguards offered by law and relevant business practices. Nevertheless, the European response to the question of whether U.S. privacy standards are adequate has been one of skepticism.[117]

---

[116] European Directive, art. 26.

[117] For a report on the EU's views, see, e.g., Thomas Weyr, *US-Europe Privacy Truce Buys Time, But EU May Target Directive Violators Early,* DMNews Int'l, Nov. 9, 1998, at 1. To make matters more complicated, the EU Directive's provisions on data transfers are enforced by the Member States, which makes their current views and future action of critical importance. See *U.S.-EC Deal on Data Privacy No Guarantee of Peace with Member States, Expert Says*, 67 U.S.L.W. 2367 (Dec. 22, 1998).

The European Union views data privacy as a fundamental right that is best protected by legislation and federal policing. The United States, in contrast, relies largely on a self-regulatory approach to effective data privacy and protection. It was inevitable that this underlying difference in ideologies would lead to a confrontation between the European Union and the United States regarding the transfer of personal data. The cornerstone of this struggle lies in Article 25 of the European Union Directive. This Article prohibits data transfers to any country lacking an "adequate" level of protection, as determined by the European Union. In the European Union's opinion, the United States is one country that does not meet its standards for the protection of data privacy.

In response to EU pressure, the Commerce Department has drafted "safe harbor" standards for privacy.[118] U.S. and European officials had been trying to reach a compromise that would create certainty for, and prevent blockage of data flow to, U.S. companies. The European Union member states agreed to a "standstill" while talks continued between the European Commission and the Clinton Administration. On March 29, 2000, the EU informally agreed to Commerce's safe harbor principles.[119]

The Commerce Department's safe harbors principles include notice to individuals about an organization's data collection practices, the ability for individuals to opt-out of such collection practices, the responsibilities of data-collecting organizations regarding the onward transfer of such data to third parties, the security and integrity of data collected, the ability of individuals to access information collected about themselves, and enforcement procedures.[120] U.S. organizations

---

[118] The International Safe Harbor Privacy Principles and comments on them are available on the Web site of the Department of Commerce's International Trade Administration, Electronic Commerce Task Force <http://www.ita.doc.gov/td/ecom/menu1.html>. For criticisms of these principles, see *Commerce's Safe Harbor Effort Praised, But Beneficiaries Want Latest Draft Tweaked*, 17 Int'l Trade Rep. (BNA) 691 (May 4, 2000); *Administration Diplomacy on Data Privacy May Not Satisfy FTC's Policy Expectations*, 67 U.S.L.W. 2331 (Dec. 9, 1998).

[119] *EC Approves U.S. Safe Harbor Principles as Consistent with EU Data Privacy Rule*, 17 Int'l Trade Rep. (BNA) 569 (April 6, 2000); *U.S., EU Leaders Expected to Endorse Privacy Protection Pact Later This Month*, 17 Int'l Trade Rep. (BNA) 727 (May 11, 2000).

[120] The "Safe Harbor Principles" are:

1) *Notice*: An organization must inform individuals about what types of information it collects about them, how it collects that information, the purposes for which it collects such information, the types of organizations to which it discloses the information, and the choices and means the organization

may qualify for the safe harbor in one of three ways: 1) by participating in a private sector privacy program which adheres to the principles; 2) if the organization is governed by statutory, regulatory, or administrative regimes which effectively protect personal data privacy, it may qualify; 3) by incorporating adequate safeguards into contracts governing transfers of personal data between[121] Companies choosing not to avail themselves of the safe harbor run the risk of not being able to receive data from sources in the European Union.[122] The Commerce Department has made clear that the principles are intended solely for U.S. organizations receiving personal data from the European Union for purposes of qualifying for the safe harbor, and that the principles are not intended to govern or affect U.S. privacy regimes addressed by government or industry efforts.

---

offers individuals for limiting its use and disclosure.

2) *Choice*: An organization must give individuals the opportunity to choose (opt out choice) whether and how personal information they provide is used.

3) *Onward Transfer*: Individuals must be given the opportunity to choose the manner in which a third party uses the personal information they provide.

4) *Security*: Organizations creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability for its intended use and must take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

5) *Data Integrity*: An organization must keep personal data relevant for the purposes for which it has been gathered only. To the extent necessary for those purposes, the data should be accurate, complete, and current.

6) Access: Individuals must have reasonable access to information about them derived from non-public records that an organization holds and be able to correct or amend that information where it is inaccurate.

7) *Enforcement:* Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals, and consequences for the organization when the principles are not followed.

[121] Europe and the U.S. International Safe Harbor Privacy Principles (draft dated April 19, 1999)<http://www.ita.doc.gov/ecom/shprin.html>.

[122] The full set of safe harbor documents constituting the U.S.-EU agreement on data privacy may be seen on the Commerce Department's Web site at <http://www.doc.gov>.

European officials have acceded to U.S. insistence upon self-regulation, and that U.S. and EU negotiators are hoping to reach final agreement by December 1999.

The EU's Data Protection Directive is only part of a larger international effort at privacy protection. For example, countries in Latin America which are developing information privacy laws include Argentina, Brazil, and Chile.[123] As part of the international effort at improving privacy in cyberspace, Germany has enacted the Teleservices Data Protection Act of 1997.

Canada, like the United States, has attempted to protect the personal identifiable information of its citizens through industry self- regulation.[124] Unlike the United States, however, Canada has established a voluntary national standard for the collection and use of personal identifiable information.[125] Currently, Canada is attempting to protect its citizens' personal identifiable information further by codifying privacy protection principles that would apply to the Internet.[126]

---

[123] Alastair Tempest, *The Globalization of Data Privacy*, DMNEWS INT'L, Mar. 15, 1999, at 5. For a survey of Internet privacy regulation in other countries, see David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL COMPUTER & INFO. L. 1 (1999).

[124] See Colin J. Bennett, *The Canadian Standards Association Model Code for the Protection of Personal Information: Reaching Consensus on Principles and Developing Enforcement Mechanisms, in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 157, 157 (U.S. Dep't Commerce, 1997) (explaining that Canada, with the exception of Quebec, has traditionally protected privacy of information in the private sector by implementing voluntary codes of fair information practice principles).

[125] See Model Code for the Protection of Personal Information, CAN/CSA- Q830-96 (Canadian Standards Ass'n 1996) (providing a standard voluntary code for the management of personal identifiable information by Canadian businesses), available at <http:// www.bild.acad.bg/dataprCa.htm>. The Canadian Standards Association is the premier "standards development and certification organization" in Canada. See Bennett, *supra* note 124, at 157.

[126] See Bill C-54, Personal Information Protection and Electronic Documents Act, 1st Sess., 36th Parl., 1996 [hereinafter Bill C-54] (proposing "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed"), available at <http:// www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C54_2/90052bE. html>.

Moving in the direction of virtually no e-mail privacy, a bill is near passage in the UK Parliament that will give investigatory authorities unlimited power to monitor and access e-mail. The Regulation of Investigatory Powers bill will enable police and security services to penetrate the operations the operations of Britain's 200 ISPs.[127] The Home Office will require ISPs to install and pay for "hardwire" links to security facilities, enabling security operators to download Internet and e-mail traffic..

V. Industry Self-Regulation

In its 1997 paper, *Global Framework for Electronic Commerce*, the Clinton Administration advocated industry self-regulation to protect consumer information online. In July 1998, however, Vice President Gore called for an "Electronic Bill of Rights" and urged Congress to pass legislation to prevent identity theft and protect medical and financial information. In regard to on-line privacy protection, then, the United States currently follows a policy of industry self-regulation.[128]

Several industry trade organizations have developed self-regulation privacy guidelines in an effort to encourage self-regulation and to avoid federal legislation. The 1999 FTC report highlighted the Online Privacy Alliance (OPA), a cross-industry coalition of corporations and associations formed in large part to encourage industry self-regulation. Although OPA does not enforce its standards on members or others, it is notable both because of its strong support for privacy seal programs and because it has helped define the commercial standards for privacy policies under a self-regulatory framework. OPA's focus is on the adoption and posting of privacy policies by commercial entities. OPA has created guidelines for privacy policies that closely resemble the FTC's fair information practices. With respect to enforcement, the OPA recommends a verification and monitoring program, a complaint resolution program, education, and outreach. The OPA favors the development of privacy seal programs to maintain the self-regulatory framework. The Online Privacy Alliance, for instance, posts model policies on its Web site, along with suggestions for a private industry enforcement framework.[129]

---

[127] See *UK moving to open all (e-)mail*, CHRISTIAN SCI. MONITOR, May 8, 2000, at 1, 9.

[128] See Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?* 48 CATH. U.L. REV. 1183 (1999); Tom Regan, *Privacy protection – or fox in the hen house*, CHRISTIAN SCI. MONITOR, April 20, 2000, at 19.

[129] Information on the OPA is available at <wwwprivacyalliance.org>. See generally Courtney Macavinta, *Net Industry Reacts to FTC Threat* <http://www.news.com/News/Item/0,4,22762,00.html> (discussing the submission of a nine-point privacy protection plan to President Clinton by twelve high-tech trade groups representing more than 11,000 companies); *Industry Presses For On-line Privacy Self-Regulation*, POST-NEWSWEEK BUS. INFO., INC., July 21, 1998, available in LEXIS,

The Direct Marketing Association has implemented an automated "privacy policy generator" on its Web site (www.the-dma.org), allowing users to create privacy policies in realtime online. The World Wide Web Consortium has defined a "Platform for Privacy Preferences" ("P3P"), a technical specification which enables web users to make informed decisions about which sites to access. According to the P3P standard, participating Web sites would register their privacy policies and users would specify various preferences. Sites that conform to the user's preferences could be accessed immediately by the user; non-conforming sites would first generate a notice, allowing the user to decide whether to continue browsing that site. BBBOnline (Better Business Bureau) works to promote the appropriate use of personal data by requiring participating Web sites to disclose their collection process to users. BBBOnline will also investigate complaints from consumers who suspect their privacy rights have been abused by a member Web site.[130]

Privacy seal programs operate like a seal of approval. Web site operators that agree to meet specified privacy standards and to be subject to an enforcement mechanism are entitled to display the program's seal on their Web site. Although privacy seal programs incorporate standards similar to the FTC fair information practices and the OPA guidelines, some use slightly different standards. Privacy seal programs are proving popular with the online business community, not only because the programs may help forestall privacy regulation, but also because consumers gain assurance from the presence of a recognized privacy seal. Three independent privacy seal programs have gained prominence:

1. *TRUSTe.* As of July 1999, almost 800 Web sites display the TRUSTe Trustmark seal. TRUSTe is a not-for-profit corporation that emerged from the West Coast technology hub to become a national privacy seal program. The TRUSTe program has evolved with generally accepted privacy standards, moving from a program based solely on disclosure of privacy policies to one that meets the OPA guidelines by requiring user choice, data security, and access. TRUSTe has a separate children's seal program that applies specifically to Web sites directed at or used by children under age thirteen. TRUSTe investigates and monitors Web sites and will investigate user complaints about practices that are not consistent with a site's privacy policy. In general, a Web site that displays the TRUSTe seal but violates the privacy policy is subject to on-site audits performed by third parties, to revocation of the right to use the seal, and to referral to the Federal

---

News Library, Curnws File (describing a broad-based coalition of on-line companies and associations proposed framework to enforce on-line privacy).

[130] See *U.S. Still Pushing for Self-Regulation of the Internet Regarding Privacy Issues,* REUTERS (Apr. 9, 1999); Communications Media Center at New York Law School, <http://www.cmcnyls.edu/public/bulletins/usspsrip.html-ssi>.

Trade Commission or other appropriate law enforcement agencies.[131]

TRUSTe also has a special "Children's Privacy Seal Program", which essentially models the Children's Online Privacy Act. As a token of compliance with the standards established by TRUSTe, a licensed corporate web-site may display the TRUSTe logo showing that due regard is given on that Web site for privacy. Among the companies that have chosen to adhere to the TRUSTe standards and display the label are: ABC News, IBM, Disney, eBay, Excite, AOL, Acer, HotMail, InfoSeek, Microsoft, Netscape, and Intel.

Of course, the TRUSTe standards are not legally binding. Under the Children's Online Privacy Act, adherence to voluntary standards, such as those established by TRUSTe, has the effect of creating a "safe harbor". This "safe harbor", however, is limited by the scope of the Children's Online Privacy Act. The FTC could still choose to exercise its Federal Trade Commission Act Section 5 authority to file actions for unfair and deceptive business practices in connection with issues surrounding collection and use of personal information collected from adults.

2. *BBBOnLine*. BBBOnLine, a subsidiary of the national Council of Better Business Bureaus, was launched in March 1999. As of July 1999, about forty Web sites display the BBBOnLine seal. Many of the initial sponsors of TRUSTe are also sponsors of BBBOnLine. BBBOnLine has set up a complaint resolution program for violations of privacy policies. As with TRUSTe, available sanctions for violating a privacy policy include revocation of the BBBOnLine seal and referral to a law enforcement agency. BBBOnLine also monitors sites and is considering a third-party verification program.[132]

3. *CPA WebTrust*. This is a more specialized privacy seal program offered by the American Institute of Certified Public Accountants in conjunction with the Canadian Institute of Chartered Accountants. The CPA WebTrust seal certifies not only that the business meets specified criteria and standards for information protection and privacy, but also that the company fulfills customer orders and fully discloses its business practices. Unlike the TRUSTe and BBBOnLine programs, which are administered by members of those organizations, the CPA WebTrust program is administered by independent auditors. The seal is licensed to independent practitioners who audit Web sites; they award the CPA WebTrust seal of assurance to sites that meet the program's standards. The CPA WebTrust program's enforcement mechanism includes mandatory arbitration of disputes concerning privacy. Because the CPA WebTrust program addresses a broader category of business practices than just privacy practices, the program may subject individual business practices to greater scrutiny and restrictions than either TRUSTe or

---

[131] Information on the TRUSTe program is available at <http:// www.truste.org>.

[132] Information on the BBBOnLine program is available at <http:// www.bbbonline.com>.

BBBOnLine. For the time being, therefore, CPA WebTrust's appeal is likely to be limited. As of July 1999, approximately twenty Web sites have been awarded the CPA WebTrust seal.[133]

To date, the most successful industry attempt at self-governance appears to be the certification program implemented by TRUSTe, an independent, non-profit organization founded by the Electronic Frontier Foundation and the CommerceNet Consortium. TRUSTe's program certifies Web sites of companies committed to complying with its privacy and disclosure practices. Certified sites are licensed to display the TRUSTe seal online.

The majority of sites do not participate in these programs. TRUSTe had only about 800 members as of July 1999, although this included many of the largest sites such as Yahoo! and Microsoft. BBBOnline, which started in March 1999, had fewer than 100 approved participants as of August 1999, although members included several large companies such as Amazon and Dell Computers. Both Microsoft Explorer and Netscape Navigator give the user the option of setting a preference that alerts the user each time a site tries to send a cookie. The user can choose to refuse the cookie but still enter the Web site. There are also companies that have developed software that either blocks cookies or allows the user to set cookie preferences.

Increasingly, individual companies, including many Internet heavyweights, are using their influence to encourage their business partners to adopt privacy policies or defined privacy practices. Several have begun to bind customers and information suppliers contractually to meet specified industry or regulatory privacy guidelines. For example, America Online, Inc. (AOL) requires AOL Certified Merchants to post privacy policies that adhere to the OPA guidelines. IBM, Microsoft, and Disney have announced that they will no longer advertise on Web sites that do not adhere to fair information practices. Such announcements are likely to carry great weight with Web site owners that depend on the growing stream of revenue from online advertising.

The FTC's 1998 *Report to Congress on Privacy On-line* was highly critical of the effectiveness of self-regulation as a means of protecting privacy on the Internet. Of the 1,400 Web sites examined by the FTC, only 14% informed visitors of their information collection practices. Despite this lack of notice, 85% percent of these sites collect personal information. Furthermore, only 2% of the Web sites examined posted a comprehensive privacy policy. The results regarding children's sites are even more unsettling. Of the 212 children's sites surveyed, 89% collected personal information from youngsters, and only about half provided some disclosure of their practices. Additionally, only 23% of the sites advised children to obtain permission before releasing their personal information; a meager 8% promised to notify parents of data collection practices; and less than 10% gave parents control over the harnessing and use of their children's data. These statistics indicate that the FTC's conclusion, that the on-line industry's privacy efforts

---

[133] Information on the CPA WebTrust program is available at <http://www.cpawebtrust.org>.

fallen "short" of what is needed, is a vast understatement.

On June 23, 1998, Commerce Secretary, William M. Daley, warned the on- line industry that "if the private sector won't ensure consumers their privacy is protected on-line, then the federal government will step in and try."[134] Likewise, Robert Pitofsky, Chairman of the Federal Trade Commission, stated that "unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary."[135]

In April 2000, in a move to head off government attempts to legislate privacy protection for Internet users, a group of 26 companies created an international industry advocacy group called the Personalization Consortium. The group describes itself as an advocacy group formed by businesses to promote the responsible and beneficial use of technology for personalizing consumer and business relationships.[136]

VI. Self-Help

With the uncertainties the Internet has generated in traditional privacy law, it might be wise to protect one's privacy with cyber-generated tools such as encryption. Encryption allows an individual, using a cryptographic algorithm and a key, to turn a message into gibberish. Once the message is sent to the intended recipient, the gibberish is decoded and becomes readable. The strongest type of safeguard is public key encryption, where whatever has been encoded with one key can be decoded only by the person with its complement. This encryption method is used by Web browsers to enable confidential transmission of credit card numbers. Of course, the ability to transmit "secret" messages makes it easier to send harmful or criminal communications. The government will want to ensure that it has a way to decode encrypted messages obtained with a warrant.[137]

---

[134] *Protect Privacy or Feds Will - Daley*, POST-NEWSWEEK BUS. INFO., INC., June 23, 1998, available in LEXIS, News Library, Curnws File.

[135] Mark Suzman, *FTC Chief Warns of Internet Privacy Action*, FIN. TIMES LIMITED (London), July 22, 1998, at 3.

[136] See Tom Regan, *Privacy protection – or fox in the hen house*, CHRISTIAN SCI. MONITOR, April 20, 2000, at 19.

[137] See, e.g., Bernstein v. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999)(mathematician's encryption software, in its source code form and as employed by those in the field of cryptography, is expression for First Amendment purposes; mathematician could bring facial challenge against regulations on prior restraint grounds; and Commerce Dep't regulations imposes prior restraint that violates First Amendment).

VII. Other Informational Privacy Acts

A. Federal Legislation

In addition to the Electronic Communications Privacy Act and the Children's Online Privacy Protection Act, Congress has enacted several other acts protecting informational privacy. These acts include:

- The Tax Reform Act, which protects the confidentiality of tax returns and return-related information and limits the dissemination of individual tax data among several federal agencies. See 26 U.S.C. § 6103 (1998).

- Freedom of Information Act, which regulates third party access to government records, including records containing personal information. See 5 U.S.C. § 552 (1998).

- Right to Financial Privacy Act, which limits government access to bank records. See 12 U.S.C. §§ 3401-34 (1998).

- Fair Credit Reporting Act, which regulates the use of credit information by credit reporting agencies. See 15 U.S.C. § 1681 (1998).

- Cable Communications Policy Act, which requires the government to possess a court order to access cable records. See 47 U.S.C. § 551 (1998).[138]

- Telecommunications Act, which safeguards customer information held by telecommunications carriers. See 47 U.S.C. § 153 (1998).

- Telephone Consumer Protection Act, which regulates telemarketing practices. See 47 U.S.C. § 227 (1998).

---

[138] See In re Application of United States, 36 F. Supp. 2d 430 (D. Mass. 1999)(granting Government's application for order directing cable television operator-ISP to disclose information regarding certain subscribers, despite conflict between Cable Communications Policy Act provision imposing liability on cable operator for disclosing personally identifiable subscriber information without notifying subscriber and Electronic Communications Privacy Act section providing that no notice was required for disclosure of records related to ISP subscriber's electronic communications).

• Federal Records Act, which regulates the disposal of federal records. See 44 U.S.C. §§ 2101-2118 (1998).

• Economic Espionage Act of 1996, 18 U.S.C. § 1832(2). The EEA criminalizes theft of trade secrets, even if the secret electronic files are copied onto a diskette owned by an employee.

• Mail Privacy Statute, 39 U.S.C § 3623.

• Privacy Act of 1974, 5 U.S.C. § 552a.[139]

• Privacy Protection Act of 1980, 42 U.S.C. § 2000aa et seq.

Provisions in the Telecommunications Act of 1996[140] and the Cable Communications Policy Act of 1984 which might apply to ISPs have not been tested.[141]

B. State Statutes and Common Law

1. State Common Law Claims

---

[139] See Barry v. Dep't of Justice, 63 F. Supp. 2d 25 (D.D.C. 1999)(Office of the Inspector General for the Department of Justice (OIG-DOJ) did not "disclose" report critical of former government employee, within meaning of Privacy Act, by posting the report on the OIG's Internet web site, where the report had already been fully released to the media and discussed in a Congressional hearing, though some Internet users might encounter the report for the first time on the OIG web site).

[140] See 47 U.S.C. § 222(f)(1) (1994) (Telecommunications Act's provisions for Customer Proprietary Network Information (CPNI)). See generally U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999)(invalidating FCC regulations that required telecommunications companies to obtain approval from customer before company uses customer's "customer proprietary network information" (CPNI) for marketing purposes because they fail to advance FCC's asserted interests in privacy and increased competition).

[141] See 47 U.S.C. § 522(7) (1994) (Cable Communications Policy Act's provisions for "cable system"). As currently interpreted, this statute is not likely to be extended to ISPs. See United States v. Kennedy, 81 F. Supp. 2d 1003 (D. Kan. 2000)(even if the government obtained defendant's subscriber information from ISP in violation of the Cable Communications Policy Act, the statute affords him no suppression remedy). See also PETER W. HUBER, THE TELECOMMUNICATIONS ACT OF 1996 54-55 (1996).

There are few reported cases involving Internet-related claims based on common law causes of action for fraud, negligent misrepresentation, invasion of privacy, or other state law theories.[142] Nevertheless, fraud and negligent misrepresentation claims would appear to be available, depending on the facts of the case. As long as the plaintiff could establish a false or misleading statement in the web site concerning the use to which personal information is to be put, reliance on the statement, and damage resulting therefrom, the cause of action would be stated. Under a fraud theory, an omission of a material fact could also be actionable. A claim based on violation of the right to privacy guaranteed by a state constitution would appear to be facially valid.

The problem with applying state law to the Internet and the collection of information in corporate web sites is that proof of the elements of these causes of action may be difficult. For example, the failure of a corporate web site to disclose the uses to which information will be put may not constitute a "false" or "misleading statement". A plaintiff would have to prove that the omission of information was misleading. This could be difficult, and would be subject to the argument that, in the absence of any affirmative misrepresentation, a reasonable user of the Internet should assume that there is no limitation on the use of information provided. Furthermore, the plaintiff would have to show both reliance and damage, two elements that might be difficult to establish.

2. State Statutes

---

[142] See, e.g., America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va.. 1998)(under Virginia law, web site operators' transmission of unsolicited bulk e-mails to customers of Internet service provider, using provider's computers and computer network, constituted trespass to chattels); Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998)(subscriber's action against ISP alleging violation of ECPA, breach of contract, breach of express and implied warranties, negligence fraud and misrepresentation, and invasion of privacy arising out of provider's disclosure of her identity pursuant to subpoena did not constitute breach of contract or of express and implied warranties; subscriber could not bring action for invasion of privacy and failed to plead fraud and misrepresentation claim with sufficient particularity); Zeran v. Diamond Broadcasting, Inc., 203 F.3d 714, 720 (10th Cir. 2000)(conduct of radio talk show hosts in accepting at face value a hoax internet electronic bulletin board posting advertising items with slogans glorifying bombing of Oklahoma City federal building, and failing to verify its authenticity before reading the listed phone number over air and encouraging listeners to call the number, did not meet the standard of recklessness required to recover for false light invasion of privacy under Oklahoma law).

Several states have enacted the following legislation either to study or regulate Internet use. Many states are also considering bills relating to Internet privacy (listed below). Attempts by the states to regulate privacy on the Internet would arguably encounter preemption difficulties under the Commerce Clause, given the interstate and international conduct involved. There is, for example, an explicit preemption clause in the Children's Online Privacy Protection Act.

1. *Arizona*: Study Committee on Internet privacy, jurisdiction, regulation, and taxation, Ariz. Rev. Stat. § 38-621 (1999).

2. *Illinois*: Advisory Commission on Internet Privacy Act, Ill. Stat. Ch. 20, § 3902/1 (1998).

3. *Maryland*: State Finance Board, powers expanded to include (a) developing standards concerning Internet-based commerce, (b) developing standards concerning Internet user privacy, (c) making recommendations concerning Internet-based crime, (d) and making recommendations concerning the use of the Internet in the health care industry. Md. Stated Fin. & Proc. § 3-409 (1999).

4. *Utah:* Government products and services on the Internet (directing state agencies to make state products and services available on the Internet by July 1, 2002), Utah Comp. Acts § 63D-1-105 (1999).

5. *Virginia*: (a) Internet use policies of library boards and other governing bodies, Va. Stat. § 42.1-36.1 (1999).

(b) 2000 Virginia House Bill 513, Internet Privacy Policy. Directs every public body that has an Internet web site to develop an Internet Privacy Policy and an Internet Privacy Policy Statement by 12/1/2000. Signed by the Governor, April 4, 2000.

The following state analogues to the ECPA provide statutory protection with regard to stored wire and electronic communications:

Ariz. Rev. Stat. Ann. § 13-3012 (1993)
Cal. Penal Code §§ 630-632 (West 1986 & Supp. 1996)
Colo. Rev. Stat. § 18-9-305 (West 1993)
Conn. Gen. Stat. Ann. §§ 53a- 187 to 53a-189 (West 1994)
Del. Code Ann. tit. 11, § 1336 (1993)
D.C. Code Ann. § 23-542 (1993)
Fla. Stat. ch 934.03 (1993)
Ga. Code Ann. § 16-11-66 (Michie 1993)
Haw. Rev. Stat. § 803-42 (1993)
Idaho Code §§ 18-6702; 18-6720

Iowa Code Ann. § 8082.B (1993)
Kan. Stat. Ann. § 21-4001; §22-2514
La. Rev. Stat. Ann. § 15:1303 (1992)
Md. Code Ann. Cts. & Jud. Proc. § 10-402 (1993)
Mich. Comp. Laws Ann. § 750.539d (West 1991)
Minn. Stat. § 626A.02 (1993)
Miss. Code Ann. § 41-29-531 (1993)
Mo. Ann. Stat. § 542.402 (Vernon 1992)
Neb. Rev. Stat. § 86-702 (1994)
Nev. Rev. Stat. § 200.620 (1993)
N.H. Rev. Stat. Ann. §§ 570-B:3; 570-A:2 (1993)
N.J. Rev. Stat. § 2A:156A-4 (1994)
N.M. Stat. Ann. § 30-12-1 (Michie 1994)
N.D. Cent. Code § 12.1-15-02 (1993)
Ohio Rev. Code Ann. § 2933.52 (Anderson 1994)
Okla. Stat. tit. 13, § 176.4 (1993)
Or. Rev. Stat. § 165.543 (1993)
Pa. Cons. Stat. Ann. § 5704 (1993)
R.I. Gen. Laws § 11-35-21 (1993)
Tex. Penal Code § 16.02 (West 1994)
Utah Code Ann. § 77-23a-4 (1994)
Va. Code Ann. § 19.2-62 (Michie 1994)
W. Va. Code § 62-1D-3 (1994)
Wis. Stat. § 968.31 (1993)
Wyo. Stat. § 7-3-602 (1994)

3. State Bills

The following bills have been introduced in state legislatures during 1999 and in the first quarter of 2000:

1. *Alaska*: 1999 House Bill 410. Relates to the crime of unauthorized interception and distribution of electronic messages; relates to privacy of information provided to and electronic messages handled by Internet service providers.

2. *California*: (a) 1999 Assembly Bill 1793, Internet Privacy Protection Act of 2000. Enacts the Internet Privacy Protection Act of 2000, which provides that no Internet service provider that provides direct Internet access services to residents of California shall disclose any personally identifying information about a California subscriber any of its affiliates, as defined, or to a 3rd party or parties for marketing or other purposes without the knowledge and affirmative consent of that subscriber.

(b) 1999 Assembly Bill 1007, Regulation of Consumer Marketing Practices. Regulates various consumer marketing practices, as specified, and imposes specified consumer notice and consent requirements on the disclosure of personal information concerning individual customers by various businesses and entities, including telephone and telegraph corporations, credit card issuers, bookkeeping services, and video rental services; enacts the Internet Privacy Protection Act of 1999.

3. *Colorado*: 2000 House Bill No. 1459, Internet Privacy Protection . Concerns privacy protection for users of the Internet; prohibits the collection or transfer of information about consumers who visit World Wide Web sites or transact business on the Internet unless the business that seeks to collect or transfer the information first, discloses the fact that the information is being collected, discloses the purpose for which the information is being collected and gives the consumer the option to decline to allow the information to be collected.

4. *Illinois*: 1999 House Bill 4622, Internet: Restroom. Amends the Criminal Code; provides that it is unlawful for any person to disseminate on the Internet any images of another person in a restroom without that other person's consent; provides that the penalty is a Class A misdemeanor.

5. *Kansas*: 1999 House Bill 2896, Internet Privacy Protection Act. Internet Privacy Protection Act; prohibits certain Internet service providers from disclosing personally identifying information about certain subscribers.

6. *Michigan*: 1999 House Bill 4171, Internet Privacy Act. Relates to computers; establishes the Internet Privacy Act.

7. *Minnesota*: 1999 Senate File 3588, Internet Privacy Policy. Relates to data practices; requires the development of a model online privacy notice; provides an Internet privacy policy for state and local governments; restricts the release of personal information.

8. *New York*: (a) 1999 Assembly Bill 9401, Internet Privacy Laws. Enacts New York State Internet Privacy Law to which operators of web sites may voluntarily be subject; limits disclosure of personal information to those submitting to the law by publicizing that they comply with such law.

(b) 1999 Senate Bill 5590, 1999 Assembly Bill 8130, Internet Privacy Practices For State Customers. Enacts the Internet Privacy Practices which prescribe measures for customers of state agencies vis a vis Internet and web site information applicable to them.

9. *Oklahoma*: 1999 House Bill 1651, Internet Privacy Protection. Creates the Consumer Internet Privacy Protection Act.

10. *Tennessee*: (a) 1999 House Bill 3115, Privacy Protection Act of 2000 for Internet Use. Relates to Internet; enacts Privacy Protection Act of 2000.

(b) 1999 House Bill 2665, Internet. Enacts "Internet Personal Information Privacy Act of 2000".

(c) 1999 Senate Bill 2360, Tennessee Internet Personal Information Privacy Act of 2000. Safeguards the privacy of personal data held by on-line computer services about their subscribers.

VIII. Proposed Legislation in the 106th Congress

Despite the growth rate of privacy seal programs and the FTC's conclusion in its 1999 report that legislation is not appropriate, the urge to regulate online activity remains strong. FTC Commissioner Orson Swindle may have said it best, in his concurring statement to the 1999 report:

> In the event that our joint efforts [with industry, privacy advocates and consumer advocates] do not produce results, I would caution industry that there are many eager and willing to regulate. If industry wants to have the freedom to adopt privacy policies in response to market incentives and not government regulation, I encourage industry to continue to lead the way.[143]

Internet-related bills are proliferating in Congress. While many seek to regulate the Internet and Internet-related activities, it is notable that many others seek to prohibit regulation of the Internet to preserve its stellar growth. To highlight the current areas of Internet-related legislative activity, the following is a list of some of the more notable:

A. Senate and Senate-House Bills

- S. 97, H.R. 368, the Children's Internet Protection Act, mandates use of filtering software for schools and libraries receiving "e-rate" funding.

- S. 328 makes permanent the moratorium on the imposition of taxes on the Internet.

- S. 393, the Congressional Openness Act, provides Internet access to Congressional documents, including certain Congressional Research Service publications, Senate lobbying and gift report filings, and Senate and joint committee documents;

- S. 637, H.R. 1245, the Internet Gun Trafficking Act of 1999, regulates the sale of firearms over the Internet.

- S. 692, the Internet Gambling Prohibition Act, prohibits gambling over the Internet.

---

[143] 1999 FTC Report (separate statement of Commissioner Orson Swindle).

• S. 699, H.R. 612, the Telemarketing Fraud and Seniors Protection Act, protects the public, especially seniors, against telemarketing fraud and fraud over the Internet. S. 699 would also direct the Federal Trade Commission to initiate a rulemaking to apply its statutory powers to deceptive acts or practices, among others, involving the initiation, transmission, and receipt of unsolicited commercial electronic mail.

• S. 759, the Inbox Privacy Act of 1999, regulates transmission of unsolicited commercial e-mail. S. 759 would require valid contact information in unsolicited commercial e-mail messages, prohibit the forgery of headers and require the honoring of "remove" requests. ISPs would be required to maintain and make available lists of users who had requested to receive any and all unsolicited commercial e-mail and would have to allow their users to "opt out" of their blocking of unsolicited commercial e-mail.

• S. 761, H.R. 1320, the Millennium Digital Commerce Act, promotes and sets standards for the use of digital signatures.

• S. 798, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROJECT) Act of 1999, described as a bill to promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national security.

• S. 809, the Online Privacy Protection Act, requires privacy disclosures on Web sites, allows consumers to "opt-out" of giving information to third parties, allows consumers to access own personal data. S. 809 would require Web site operators to provide notice regarding the type of personal information and how it is used and disclosed; and require users to consent to or limit disclosure of such information.

• S. 854, the Electronic Rights for the 21st Century Act, described as a bill to protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to location information, decryption assistance for encrypted communications and stored electronic information and other information; and to affirm the rights of Americans to use and sell encryption products as a tool for protecting their online privacy.

• S. 1043, the Internet Regulatory Freedom Act of 1999, deprives the Federal Communications Commission of jurisdiction to set standards for the Internet.

• S. 1255, H.R.3028, the Anticyber-squatting Consumer Protection Act / Trademark Cyberpiracy Prevention Act, is designed "to protect consumers and promote electronic commerce by amending certain trademark infringement, dilution, and counterfeiting laws." It was signed into law on November 30, 1999.

• S. 1461, the Domain Name Piracy Prevention Act of 1999, prohibits "the bad-faith registration, trafficking or use of Internet domain names that are identical to, confusingly similar to, or dilutive of distinctive trademarks or service marks."

• S. 1545, the Neighborhood Children's Internet Protection Act, requires schools and libraries receiving universal service assistance to install systems or implement acceptable use policies for blocking or filtering Internet access to matter inappropriate for minors, requires a study of available Internet blocking or filtering software).

• S. 1901, the Privacy Protection Study Commission Act of 1999, establishes a Privacy Protection Study Commission to evaluate the Freedom of Information Act and E-FOIA.

B. House Bills

• H.R. 87 prohibits Internet and mail order sales of ammunition without a license to deal in firearms; requires licensed firearms dealers to record all sales of 1,000 rounds of ammunition to a single person.

• H.R. 313, the Consumer Internet Privacy Protection Act of 1999, regulates the use by interactive computer services of personally identifiable information provided by subscribers.

• H.R. 367, Social Security On-line Privacy Protection Act of 1999, would require operators of interactive consumer services to request permission from consumers to disclose Social Security numbers or related personally identifiable information to third parties.

• H.R. 369, Children's Privacy Protection and Parental Empowerment Act of 1999, would require operators of interactive consumer services to request permission from consumers to disclose personally identifiable information to third parties.

• H.R. 439, the Paperwork Elimination Act of 1999, promotes the use of digital signatures in submission of government documents.

• H.R. 654, the Congressional Research Accessibility Act, makes available on the Internet, for purposes of access and retrieval by the public, certain information available through the Congressional Research Service Web site.

• H.R. 850, the Security and Freedom Through Encryption Act, affirms the right to use and sell encryption, liberalizes export controls, and prohibits domestic key recovery.

• H.R. 896, the Children's Internet Protection Act, requires schools and libraries to use filtering or blocking technology on computers with Internet access to remain eligible for universal service assistance.

• H.R. 1685, H.R. 1686, the Internet Growth and Development Act / Internet Freedom Act, relaxes regulations on local phone companies for Internet traffic while requiring them to provide broadband service where possible; prohibits local phone companies from refusing to provide competitors with reasonable access to broadband-compatible local loops; requires that "broadband access transport providers" must not discriminate between unaffiliated ISPs and affiliated ISPs; prohibits false return addresses in unsolicited commercial e- mail; promotes the use of digital signatures; and requires ISPs to post and comply with privacy policies. H.R. 1685 would amend Title VII of the Communications Act of 1934 by adding a provision requiring that users comply with an ISP's unsolicited e- mail policy. H.R. 1685 gives an ISP a civil right of action to recover actual monetary loss or liquidated damages up to a maximum of $25,000 a day.

• H.R. 1714, the Electronic Signatures in Global National Commerce Act, establishes national procedural guidelines affecting electronic signatures and records, electronic record retention and interaction of electronic agents.

• H.R. 1910, the E-Mail User Protection Act, prohibits abusive use of unsolicited bulk electronic mail. H.R. 1910 would prohibit the sending of unsolicited bulk e-mail containing false information regarding sender, return address or header. It also would prohibit the initiation of unsolicited bulk e-mail if the recipient has previously requested that such messages not be sent. A violator of the act would be fined $50 per message or $10,000 per day.

• H.R. 2162, the Can Spam Act, prohibits the use of the equipment of an electronic mail service provider to send unsolicited commercial electronic mail in contravention of the provider's posted policy; prohibits unauthorized use of Internet domain names. H.R. 2162 would give ISPs a right of action against spammers who violate an ISP's anti-unsolicited commercial e-mail policy. It also would create criminal penalties for hijacking the domain names of others in sending unsolicited commercial e- mail.

• H.R. 2560, the Child Protection Act of 1999, requires public schools and libraries that receive federal funds for the acquisition or operation of computers to install software to protect children from obscenity.

• H.R. 2616, the Encryption for the National Interest Act, clarifies the policy of the United States with respect to the use and export of encryption products.

• H.R. 2617, the Tax Relief for Responsible Encryption Act of 1999, amends the Internal Revenue Code to allow a tax credit for development costs of encryption products with plain text capability without the user's knowledge.

• H.R. 3113, the Unsolicited Electronic Mail Act of 1999, is designed "to protect individuals, families, and Internet service providers from unsolicited and unwanted electronic mail."

• H.R. 3125, the Internet Gambling Prohibition Act of 1999, prohibits gambling over the Internet;

• H.R. 3321, the Electronic Privacy Bill of Rights Act, requires privacy disclosures on Web sites; requires consumer "consent" for all uses of data; and allows consumers to access their own personal data.

• H.R. 3560, Internet Privacy. Requires 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; provides greater individual control over the collection and use of that information.

REPORT ON INTERVENTION OF PROSECUTING ATTORNEYS IN DIVORCE ACTIONS, M.C.L. § 552.45, AND RECOMMENDATION TO THE LEGISLATURE

In October 2000, Circuit Judge Charles W. Johnson of the 57th Judicial District wrote to the Commission to inform it of M.C.L. § 552.45. In his letter Judge Johnson wrote:

> In connection with the Law Revision Commission's obligation to examine statutes or the purpose of discovering defects and anachronisms in the law, I am writing to recommend a review of MCL 552.45.
>
> This statute appears to have been originally enacted in the 1800's. It requires that in every divorce case involving minor children, the complaint must be served on the prosecuting attorney. The prosecutor must then enter an appearance, "and when, in his judgment, the interest of the children or the public good so requires, he shall introduce evidence and appear at the hearing and oppose the granting of a decree of divorce."
>
> In my tenure as a circuit judge, there has not been one time when a prosecutor has actually appeared in a divorce case to oppose granting the divorce. Since the enactment of the no fault divorce law, I am unaware of any grounds upon which this could be done. The above statute was obviously enacted before the advent of no fault divorce. To the extent that the intent was to have some independent person or agency in divorce proceedings watching out for the interests of the minor children, that purpose is now well served by the office of the Friend of the Court.
>
> In my view, MCL 552.45 is an anachronism. It should be repealed.

The statute in issue, M.C.L. § 552.45 provides as follows:

> 552.45. Children; enumeration in complaint; notice to prosecutor or friend of court; opposition to decree, fee; interest of prosecutor or partners in case
>
> Sec. 45. Every bill of complaint filed shall set forth the names and ages of all children of the marriage, and when there are children under 17 years of age a copy of the summons issued in the cause shall be served upon the the [sic] prosecuting attorney of the county where suit is commenced, or upon the friend of the court in those counties having a population of 500,000 or more which have a friend of the court. The prosecuting attorney or friend of the court so served shall enter his appearance in the cause, and when, in his judgment, the interest of the children or the public good so requires, he shall introduce evidence and appear at the hearing and oppose the granting of a decree of divorce. In any case wherein there are no

children the issue of such marriage under the age of 17 years, when it shall appear to the court that the public good so requires, an order may be entered requiring the prosecuting attorney or friend of the court in counties having a population of 500,000 or more to appear and oppose the granting of a decree of divorce. For every case which the prosecuting attorney investigates, and in which he appears by and with the consent of the court, he shall receive the sum of $5.00, to be paid by the county treasurer upon the certificate of the circuit judge that such services have been performed. Nothing in this act contained shall be construed as preventing prosecuting attorneys or their partners from acting as solicitors or counsel for either party to the suit. If a prosecuting attorney or friend of the court is in any way interested as solicitor or counsel for either of the parties the court shall appoint some reputable attorney to perform the services of prosecuting attorney, as provided in this act, who shall receive the compensation provided for such service.

Question Presented

Should M.C.L. § 552.45 be repealed?

Recommendation

The Commission recommends that the Legislature repeal M.C.L. § 552.45.

REPORT ON THE MICHIGAN SALES REPRESENTATIVE STATUTE AND RECOMMENDATIONS TO THE LEGISLATURE

I. Scope of the Michigan Sales Representative Statute and the Awarding of Damages and Attorneys' Fees under the Statute.

A. Background.

The Michigan Sales Representative Statute (Statute), MCL 600.2961, enacted as a section of the Revised Judicature Act of 1961, provides a remedy for salespersons who, after termination of their employment, are denied commissions for sales made before their termination.

B. The *Kenneth Henes Special Products Procurement v Continental Biomass Industries, Inc.* decision.

In ***Kenneth Henes Special Products Procurement v Continental Biomass Industries, Inc.,*** 86 F Supp 2nd 721(ED Mich 2000), the United States District Court focused on the three following issues regarding the Statute:

(1) Does the Statute provide a remedy for a sales representative who entered into a sales representative contract in Michigan, if the sale for which the commission is claimed was not made in Michigan?

The pertinent language in the Statute provides:

> (1) As used in this section:
>
> ***
>
> (d) "Principal" means a person that does either of the following:
>
> ***
>
> (ii) Contracts with a sales representative to solicit orders for or sell a product in this state.
>
> MCL 600.2961(1)(d)(ii).

The Court discussed the ambiguous placement of the phrase "in this state" in MCL 600.2961(1)(d)(ii), noting that it could be read as referring to the situs at which the contract was entered into, the situs of the sale of goods, or the situs of the sales representative. After examining the legislative history of the Statute, the Court held that the Statute would apply to sales representative contracts entered into in Michigan, and, therefore, would provide a remedy to a sales representative who was a party to such a contract even if the sale for which the commission is claimed was not made in Michigan.

(2) How are damages calculated under the Statute when the intentional withholding of *several* commissions of varying amounts, some of which exceed $50,000, are at issue?

The pertinent language in the Statute provides:

> (5) A principal who fails to comply with this section is liable to the sales representative for both of the following:
>
> (a) Actual damages caused by the failure to pay the commissions when due.
>
> (b) If the principal is found to have intentionally failed to pay the commission when due, an amount equal to 2 times the amount of commissions due but not paid as required by this section or $100,000.00, whichever is less.
>
> MCL 600.2961(5).

The Court indicated that the language of MCL 600.2961(5)(b) quoted above could be interpreted as requiring any of the following possible different ways of calculating damages:

(a) The amount of each intentionally withheld commission is doubled. All of the amounts resulting from the doubling are added together to determine the amount owed under MCL 600.2961(5). If, however, the amount resulting from the doubling of any one commission is more than $100,000, the figure of $100,000 is used in regard to that commission.

Example:

Amount of intentionally withheld commissions	Amount resulting from doubling (not to exceed $100,000)	Amount calculated under MCL 600.2961(5)
$40,000	$80,000 (i)	((i) + (ii) + (iii))
$45,000	$90,000 (ii)	$270,000
$60,000	$100,000 (iii)	

(b) The amount of each intentionally withheld commission is doubled. The amounts of all intentionally withheld commissions plus the amounts resulting from the doubling are added together to determine the amount owed under MCL 600.2961(5). If, however, the amount resulting from the doubling of any one commission is more than $100,000, the figure of $100,000 is used in regard to that commission.

Example:

Amount of intentionally withheld commissions	Amount resulting from doubling (not to exceed $100,000)	Amount calculated under MCL 600.2961(5)
$40,000 (i)	$80,000 (iv)	((i) + (ii) + (iii) +)
$45,000 (ii)	$90,000 (v)	(iv) + (v) + (vi)
$60,000 (iii)	$100,000 (vi)	$415,000

(c) The amount of all intentionally withheld commissions are added together. The total is doubled. If the amount resulting from the doubling is less than $100,000, that amount is added to the total to determine the amount of the award under MCL 600.2961(5). If the amount resulting from the doubling is more than $100,000, the figure of $100,000 is added to the total to determine the amount of the award under MCL 600.2961(5).

Example:

Total of the amounts of intentionally withheld commissions	Amount resulting from doubling (not to exceed $100,000)	Amount calculated under MCL 600.2961(5) ((i) + (ii))
$40,000		
$45,000		
$60,000		
$145,000 (i)	$100,000 (ii)	$245,000

After reviewing a previous court decision and the language of similar statutes of other states, the Court held that the third option was intended, that is that the cap under MCL 600.2961(5)(b) applies cumulatively to unpaid commissions in the aggregate, and, therefore, the amount of damages under the Statute can never exceed the actual damages plus $100,000.

(3) Does the Statute provide for attorneys' fees for a party prevailing on an allegation of intentional failure to pay brought under MCL 600.2961 concerning one of several

claimed commissions even though it did not prevail on other allegations brought under MCL 600.2961 for other claimed commissions, but nonetheless prevailed in regard to those commissions on alternative theories of liability?

The pertinent language in the Statute provides:

> (1) As used in this section:
>
> ***
>
> (c) "Prevailing party" means a party who wins on all the allegations of the complaint or on all of the responses to the complaint.
>
> ***
>
> (6) If a sales representative brings a cause of action pursuant to this section, the court shall award to the prevailing party reasonable attorney fees and court costs.
>
> MCL 600.2961(1)(c)(6).

The Court, based on past precedent, held that attorneys' fees would be awarded in such an instance.

Questions Presented

1. Should the Michigan Sales Representative Statute be amended to clarify that, for purposes of determining the liability of a principal for unpaid commissions, the term "principal" includes an individual who contracts in the state of Michigan with a sales representative even if the sales take place outside of Michigan?

2. Should the Michigan Sales Representative Statute be amended to clarify the damages available for an intentional failure to pay a commission?

3. Should the Michigan Sales Representative Statute be amended to provide that attorneys' fees should not be awarded unless a party prevails on all allegations brought under the Statute?

Recommendation

1. The Commission recommends that the Sales Representative Act be amended as follows, to clarify the definition of the term "principal":

   (1) As used in this section:

   ***

   (d) "Principal" means a person that does either of the following:

   (i) Manufactures, produces, imports, sells, or distributes a product in this state.

   (ii) Contracts IN THIS STATE with a sales representative to solicit orders for or sell a product ~~in this state~~.

   ***

2. The Commission does not recommend the amendment, as it finds the current provision to be of sufficient clarity.

3. The Commission recommends that the Legislature closely consider whether the construction the Henes Court has given to MCL 600.296(1)(c) and (6) is in line with the Legislature's intent, but otherwise makes no recommendation.

RECENT COURT DECISIONS IDENTIFYING ACTS FOR LEGISLATIVE ACTION: A REPORT TO THE MICHIGAN LAW REVISION COMMISSION AND RECOMMENDATIONS TO THE LEGISLATURE

I. Introduction.

As part of its statutory charge to examine current judicial decisions for the purpose of discovering defects in the law and to recommend needed reforms, the Michigan Law Revision Commission undertook a review of three Michigan Court of Appeals' decisions released in 2000. These three cases identify Acts and a common law rule as candidates for legislative reform. The three opinions are:

Diehl v. Danuloff, 242 Mich. App. 120, 618 N.W.2d 83 (2000)(whether court-appointed psychologists enjoy immunity from suit either under the Government Tort Liability Act or under common law)

People v. Stephan, 241 Mich. App. 482, 616 N.W.2d 188 (2000)(resolution of conflict between insanity statute and guilty-but-mentally-ill statute)

In the Matter of RFF, 242 Mich. App. 188, 617 N.W.2d 745 (2000) (termination of biological father's parental rights under the Adoption Code)

II. Tort Immunity of Court-Appointed Psychologists.

A. Background.

The Government Tort Liability Act, M.C.L. § 691.1407 (GTLA) extends immunity for acts of negligence to the following categories of persons:

- officers and employees of a governmental agency
- volunteers acting on behalf of a governmental agency
- members of a board, council, commission, or task force of a governmental agency
- judges, legislators, and the elective or highest appointive executive officials of all levels of government

In *Bullock v. Huster*, 209 Mich. App. 551, 532 N.W.2d 202, *vacated and remanded*, 451 Mich. 884, 549 N.W.2d 573, *on remand*, 218 Mich. App. 400, 554 N.W.2d 47 (1996), the guardian ad litem of a minor child was sued for allegedly failing to conduct an adequate investigation prior to making a recommendation to the court. The Court of Appeals in that case found that the GTLA does not include guardians ad litem within the class of persons entitled to immunity and, accordingly, held that the intent of the Legislature was to exclude guardians ad litem from the scope of governmental tort immunity. Following an amendment to the GTLA to

extend governmental immunity to guardians ad litem, the Michigan Supreme Court reversed the Court of Appeals in *Bullock*. On remand, the Court of Appeals dismissed the lawsuit.

B. The *Diehl v. Danuloff* Decision.

As part of a custody dispute involving two children, the trial court ordered defendant Lyle Danuloff to perform a full psychological evaluation of the family unit and make a custody recommendation to the court. He recommended that the father be awarded custody of the children, which recommendation the court followed.

Subsequently, the children's grandparents brought a negligence action against Danuloff, alleging that he had conducted the custody evaluation in a negligent manner. The core of their complaint was that the children's father had been charged and convicted of sexually abusing the children.

The trial court granted summary disposition, finding *inter alia* that Danuloff was entitled to absolute immunity at common law.

In this case of first impression, the Court of Appeals, drawing on its earlier decision in *Bullock*, concluded that because court-appointed private psychologists are not expressly included within the class of persons entitled to immunity under the GTLA, that is was the Legislature's intent to exclude them.

The Court went on to examine whether court-appointed psychologists should nevertheless be accorded common law quasi-judicial immunity. In reviewing the case law in other jurisdictions, the Court found that with virtual uniformity, courts in other jurisdictions (e.g., Nevada, Utah, Alaska) have granted quasi-judicial immunity to individuals who perform functions analogous to those performed by defendant Danuloff in the present case. The Court of Appeals held, therefore, that quasi-judicial immunity extends to court-appointed psychologists ordered to conduct evaluations and make recommendations to the trial court in custody disputes.

Question Presented

Should the Government Tort Liability Act be amended to codify the holding in *Diehl v. Danuloff*?

Recommendation

The Commission recommends that the Legislature amend the Government Tort Liability Act to codify the holding in the *Diehl* decision by including court-appointed psychologists among the class of persons protected under the Act.

III. Resolution of Conflict Between Insanity Statute and Guilty-But-Mentally-Ill Statute

A. Background.

In 1994, the Legislature amended the insanity statute to require criminal defendants who assert an insanity defense to prove insanity by a preponderance of the evidence. Prior law placed the burden on the prosecutor to prove beyond a reasonable doubt that the defendant was not legally insane. However, the Legislature did not amend the guilty-but-mentally-ill (GBMI) statute in the same manner. As a consequence, when the trial court instructs the jury on the requirements of both the insanity and GBMI statutes, the instructions state that the defendant bears the burden of proving mental illness and legal insanity for an insanity verdict, but that the prosecutor bears the burden of proving lack of insanity for purposes of the GBMI statute. These instructions contradict each other and create an irreconcilable conflict for the jury trying to apply them.

B. The *People v. Stephan* Decision.

In *People v. Stephan*, the prosecutor argued before the Court of Appeals that when the Legislature amended the insanity statute in 1994, it implicitly repealed that portion of the GBMI statute that requires the prosecutor to prove mental illness beyond a reasonable doubt.

Although it was sympathetic with the plight of judges, juries, and prosecutors in resolving this statutory conflict, the Court of Appeals declined to accept the prosecutor's argument. The Court stated that "our due regard for the doctrine of separation of powers precludes our invading the province of the Legislature by inferring that any statute has been implicitly amended, repealed, or partially repealed. . . . Therefore, we defer to the Legislature to make these necessary changes."

Question Presented

Should the GBMI statute be amended to comport with the 1994 amendments to the insanity statute?

Recommendation

The Commission recommends that the Legislature examine this question and make whatever changes are necessary to resolve this statutory conflict.

IV. Termination of Biological Father's Parental Rights under the Adoption Code.

A. Background.

The Adoption Code, M.C.L. § 710.39, creates two categories of putative fathers -- "do-nothing" and "do-something" fathers -- and provides different standards for termination of the rights of each. Section 39(1) of the Adoption Code deals with the first group. Putative fathers who have established no custodial relationship with the child, and who have provided no support for the mother or child prior to the notice of hearing, may have their parental rights terminated if the court finds that it would not be in the best interests of the child to grant custody to him.

The second group is dealt with under Section 39(2) of the Adoption Code. The parental rights of fathers who have established some kind of custodial or support relationship prior to the notice of hearing may have their parental rights terminated only through proceedings under the Probate Code (in essence, termination for abuse or neglect).

B. The *In re RFF* Decision.

In *In the Matter of RFF*, the biological father argued that he was entitled to be treated as a father who had provided support to the mother or child, and thus entitled to the parental termination procedure of Section 39(2). It was undisputed that he had not established a custodial relationship with RFF. However, the biological father argued that the only reason he did not provide support to either the mother or child is that she had concealed her pregnancy from him until less than a month before the child's birth, and that the adoption agency had assured him that the costs of the pregnancy were being paid by the prospective adoptive parents.

The Court concluded that the Legislature did not consider the case of the rights of a deceived father when it amended the Adoption Code in 1998. The Court stated that "the Legislature should reexamine § 39 and evaluate whether it is appropriate to place a father who has been deceived about a pregnancy in subsection 39(1) or subsection 39(2) or whether it is appropriate to create third subsection to address this specific problem." 617 N.W.2d at 201.

In her dissent from the Supreme Court's denial of leave to appeal, Chief Justice Maura Corrigan expressed concerns over the potential equal protection defects of Sections 39(1) and 39(2) of the Adoption Code in that the Code treats putative fathers who are not deceived as to the pregnancy differently from those who are. *In re RFF*, 618 N.W.2d 575 (2000)(leave to appeal denied; Corrigan, J., dissenting).

Question Presented

Should the Legislature amend the Adoption Code to address termination of the parental rights of biological fathers who are deceived as to the existence of the pregnancy?

Recommendation

This issue presents a very complex matter that requires careful examination. The Commission, therefore, takes no position on this question at this time and makes no recommendation to the Legislature. The Commission will be studying this matter in the future.

An Update on Prior Commission Recommendations

A. Taxation of Paralegal Costs under M.C.L. § 600.2405.

In response to the Court of Appeals' decision in *Joerger v. Gordon Food Service, Inc.*, 224 Mich. App. 167 (1997)(paralegal costs not recoverable as part of an award of attorney fees), in its 1997 Annual Report the Commission recommended to the Legislature that it amend M.C.L. § 600.2405 to provide that paralegal expenses be included as an item of recoverable costs in civil litigation.

On October 24, 2000, the Supreme Court adopted Rule 2.626 of the Michigan Court Rules, effective January 1, 2001, to provide that an award of attorney fees may include an award for the time and labor of any legal assistant who contributed nonclerical, legal support under the supervision of an attorney.

B. Judicial Overruling of *Dedes v. Asch*.

In *Dedes v. Asch*, 446 Mich. 99, 521 N.W.2d 488 (1994), the Michigan Supreme Court was asked to interpret the phrase "the proximate cause" contained in the Government Tort Liability Act. The Court held in *Dedes* that the Legislature's use of the definite article *"the"* to modify the term "proximate cause" did not mean "the *sole* proximate cause." Instead, the Court interpreted the words, "the proximate cause," to mean "*a* proximate cause" of the plaintiff's injuries. Consequently, the school bus driver in *Dedes* was not immune from suit when children were hit by a passing car immediately after alighting from the school bus.

In its 1996 Annual Report, the Commission recommended legislative overruling of *Dedes v. Asch*. In 2000, the Supreme Court overruled *Dedes v. Asch* in *Robinson v. City of Detroit*, 613 N.W.2d 307. The Court held that the phrase "the proximate cause" used in the GTLA means

"the one most immediate, efficient, and direct cause preceding an injury, not 'a proximate cause.'" 613 N.W.2d at 311.

PRIOR ENACTMENTS PURSUANT TO MICHIGAN LAW REVISION COMMISSION RECOMMENDATIONS

The following Acts have been adopted to date pursuant to recommendations of the Commission and in some cases amendments thereto by the Legislature:

1967 Legislative Session

Subject	Commission Report	Act No.
Original Jurisdiction of Court of Appeals	1966, p. 43	65
Corporation Use of Assumed Names	1966, p. 36	138
Interstate and International Judicial Procedures	1966, p. 25	178
Stockholder Action Without Meetings	1966, p. 41	201
Powers of Appointment	1966, p. 11	224
Dead Man's Statute	1966, p. 29	263

1968 Legislative Session

Subject	Commission Report	Act No.
Possibilities of Reverter and Right of Entry	1966, p. 22	13
Stockholder Approval of Mortgage of Corporate Assets	1966, p. 39	287
Corporations as Partners	1966, p. 34	288
Guardians Ad Litem	1967, p. 53	292
Emancipation of Minors	1967, p. 50	293
Jury Selection	1967, p. 23	326

1969 Legislative Session

Subject	Commission Report	Act No.
Access to Adjoining Property	1968, p. 19	55
Recognition of Acknowledgments	1968, p. 64	57
Dead Man's Statute Amendment	1966, p. 29	63
Notice of Change in Tax Assessments	1968, p. 30	115
Antenuptial and Marital Agreements	1968, p. 27	139
Anatomical Gifts	1968, p. 39	189
Administrative Procedures Act	1967, p. 11	306
Venue for Civil Actions	1968, p. 17	333

1970 Legislative Session

Subject	Commission Report	Act No.
Land Contract Foreclosures	1967, p. 55	86
Artist-Art Dealer Relationships	1969, p. 41	90
Minor Students' Capacity to Borrow Act	1969, p. 46	107
Warranties in Sales of Art	1969, p. 43	121
Appeals from Probate Court	1968, p. 32	143
Circuit Court Commissioner Powers of Magistrates	1969, p. 57	238

1971 Legislative Session

Subject	Commission Report	Act No.
Revision of Grounds for Divorce	1970, p. 7	75
Civil Verdicts by 5 of 6 Jurors In Retained Municipal Courts	1970, p. 40	158
Amendment of Uniform Anatomical Gift Act	1970, p. 45	186

1972 Legislative Session

Subject	Commission Report	Act No.
Summary Proceeding for Possession of Premises	1970, p. 16	120
Interest on Judgments	1969, p. 59	135
Business Corporations	1970, Supp.	284
Constitutional Amendment re Juries of 12	1969, p. 60	HJR "M"

1973 Legislative Session

Subject	Commission Report	Act No.
Execution and Levy in Proceedings Supplementary to Judgment	1970, p. 51	96
Technical Amendments to Business Corporation Act	1973, p. 8	98

1974 Legislative Session

Subject	Commission Report	Act No.
Venue in Civil Actions Against Non-Resident Corporations	1971, p. 63	52
Choice of Forum	1972, p. 60	88
Extension of Personal Jurisdiction in Domestic Relations Cases	1972, p. 53	90
Technical Amendments to the Michigan General Corporations Act	1973, p. 37	140
Technical Amendments to the Revised Judicature Act	1971, p. 7	297

Technical Amendments to the Business Corporation Act	1974, p. 30	303
Amendment to Dead Man's Statute	1972, p. 70	305
Attachment and Collection Fees	1968, p. 22	306
Contribution Among Joint Tortfeasors	1967, p. 57	318
District Court Venue in Civil Actions	1970, p. 42	319
Due Process in Seizure of a Debtor's Property (Elimination of Pre-judgment Garnishment)	1972, p. 7	371

1975 Legislative Session

Subject	Commission Report	Act No.
Hit-Run Offenses	1973, p. 54	170
Equalization of Income Rights of Husband and Wife in Entirety Property	1974, p. 12	288
Disposition of Community Property Rights at Death	1973, p. 50	289
Insurance Policy in Lieu of Bond	1969, p. 54	290
Child Custody Jurisdiction	1969, p. 23	297

1976 Legislative Session

Subject	Commission Report	Act No.
Due Process in Seizure of a Debtor's Property (Replevin Actions)	1972, p. 7	79
Qualifications of Fiduciaries	1966, p. 32	262
Revision of Revised Judicature Act Venue Provisions	1975, p. 20	375
Durable Family Power of Attorney	1975, p. 18	376

1978 Legislative Session

Subject	Commission Report	Act No.
Juvenile Obscenity	1975, p. 133	33
Multiple Party Deposits	1966, p. 18	53
Amendment of Telephone and Messenger Service Company Act	1973, p. 48	63
Elimination of References to Abolished Courts:		
a. Township By-Laws	1976, p. 74	103
b. Public Recreation Hall Licenses	1976, p. 74	138
c. Village Ordinances	1976, p. 74	189
d. Home Rule Village Ordinances	1976, p. 74	190
e. Home Rule Cities	1976, p. 74	191
f. Preservation of Property Act	1976, p. 74	237
g. Bureau of Criminal Identification	1976, p. 74	538
h. Fourth Class Cities	1976, p. 74	539
i. Election Law Amendments	1976, p. 74	540
j. Charter Townships	1976, p. 74	553
Plats	1976, p. 58	367
Amendments to Article 9 of the Uniform Commercial Code	1975, Supp.	369

1980 Legislative Session

Subject	Commission Report	Act No.
Condemnation Procedures	1968, p. 8	87
Technical Revision of the Code of Criminal Procedure	1978, p. 37	506

1981 Legislative Session

Subject	Commission Report	Act No.
Elimination of Reference to the Justice of the Peace: Sheriff's Service of Process	1976, p. 74	148
Court of Appeals Jurisdiction	1980, p. 34	206

1982 Legislative Session

Subject	Commission Report	Act No.
Limited Partnerships	1980, p. 40	213
Technical Amendments to the Business Corporation Act	1980, p. 8	407
Interest on Probate Code Judgments	1980, p. 37	412

1983 Legislative Session

Subject	Commission Report	Act No.
Elimination of References to Abolished Courts: Police Courts and County Board of Auditors	1979, p. 9	87
Federal Lien Registration	1979, p. 26	102

1984 Legislative Session

Subject	Commission Report	Act No.
Legislative Privilege: a. Immunity in Civil Actions	1983, p. 14	27

b. Limits of Immunity in Contested Cases	1983, p. 14	28
c. Amendments to R.J.A. for Legislative Immunity	1983, p. 14	29
Disclosure of Treatment Under the Psychologist/Psychiatrist-Patient Privilege	1978, p. 28	362

1986 Legislative Session

Subject	Commission Report	Act No.
Amendments to the Uniform Limited Partnership Act	1983, p. 9	100

1987 Legislative Session

Subject	Commission Report	Act No.
Amendments to Article 8 of the Uniform Commercial Code	1984, p. 97	16
Disclosure in the Sale of Visual Art Objects Produced in Multiples	1981, p. 57	40, 53, 54

1988 Legislative Session

Subject	Commission Report	Act No.
Repeal of M.C.L. §764.9	1982, p. 9	113
Statutory Rule Against Perpetuities	1986, p. 10	417, 418
Transboundary Pollution Reciprocal Access to Courts	1984, p. 71	517

1990 Legislative Session

Subject	Commission Report	Act No.
Elimination of Reference to Abolished Courts:		
a. Procedures of Justice Courts and Municipal Courts	1985, p. 12; 1986, p. 125	217
b. Noxious Weeds	1986, p. 128; 1988, p. 154	218
c. Criminal Procedure	1975, p. 24	219
d. Presumption Concerning Married Women	1988, p. 157	220
e. Mackinac Island State Park	1986, p. 138; 1988, p. 154	221
f. Relief and Support of the Poor	1986, p. 139; 1988, p. 154	222
g. Legal Work Day	1988, p. 154	223
h. Damage to Property by Floating Lumber	1988, p. 155	224

1991 Legislative Session

Subject	Commission Report	Act No.
Elimination of Reference to Abolished Courts:		
a. Land Contracts	1988, p. 157	140
b. Insurance	1988, p. 156	141
c. Animals	1988, p. 155	142
d. Trains	1986, pp. 153, 155; 1987, p. 80; 1988, p. 152	143
e. Appeals	1985, p. 12	144
f. Crimes	1988, p. 153	145
g. Library Corporations	1988, p. 155	146
h. Oaths	1988, p. 156	147
i. Agricultural Products	1986, p. 134; 1988, p. 151	148
j. Deeds	1988, p. 156	149
k. Corporations	1989, p. 4; 1990, p. 4	150
l. Summer Resort Corporations	1986, p. 154; 1988, p. 155	151

m. Association Land	1986, p. 154; 1988, p. 155	152
n. Burial Grounds	1988, p. 156	153
o. Posters, Signs, and Placecards	1988, p. 157	154
p. Railroad Construction	1988, p. 157; 1988, p. 156	155
q. Work Farms	1988, p. 157	156
r. Recording Duties	1988, p. 154	157
s. Liens	1986, pp. 141, 151, 158; 1988, p. 152	159

1992 Legislative Session

Subject	Commission Report	Act No.
Determination of Death Act	1987, p. 13	90

1993 Legislative Session

Subject	Commission Report	Act No.
Condemnation Procedures of Home Rule Villages	1989, p. 17	32
Condemnation Procedures Regarding Railroads	1989, p. 25	354
Condemnation Procedures Regarding Railroad Depots	1989, p. 26	354

1995 Legislative Session

Subject	Commission Report	Act No.
Condemnation Procedures Regarding Inland Lake Levels	1989, p. 24	59
Condemnation Procedures of School Districts	1989, p. 24	289

1996 Legislative Session

Subject	Commission Report	Act No.
Felony Murder and Arson	1994, p. 179	20, 21

1998 Legislative Session

Subject	Commission Report	Act No.
Condemnation Procedures of General Law Villages	1989, p. 16	254
Repeal of Article 6 of the Uniform Commercial Code	1994, p. 111; 1997, p. 131	489
Uniform Fraudulent Transfer Act	1988, p. 13	434
Uniform Trade Secrets Act	1993, p. 7	448

BIOGRAPHIES OF COMMISSION MEMBERS AND STAFF

RICHARD D. McLELLAN

Richard D. McLellan, is Chairman of the Michigan Law Revision Commission, a position he has filled since 1986 following his appointment as a public member of the Commission in 1985.

Mr. McLellan is a lawyer with the law firm of Dykema Gossett PLLC and serves as the Member-in-charge of the firm's Lansing Office and as the leader of the firm's Government Policy & Practice Group. He is responsible for the firm's public policy, administrative law and lobbying practices in Lansing, Chicago and Washington, D.C.

Mr. McLellan started his career as an administrative assistant to Governor William G. Milliken and as director of the Michigan Office of Drug Abuse.

Following the 1990 Michigan elections, McLellan was named Transition Director to then Governor-elect John Engler. In that capacity, he assisted in the formation of Governor Engler's Administration and conducted a review of state programs. He has also been appointed by the Governor as Chairman of the Corrections Commission, a member of the Michigan Export Development Authority, a member of the Michigan International Trade Authority, a member of the Library of Michigan Board of Trustees and a member of the Michigan Jobs Commission.

During the administration of President Gerald Ford, he served as an advisor to the Commissioner of the Food and Drug Administration as a member of the National Advisory Food and Drug Committee of the U.S. Department of Health, Education and Welfare.

In 1990, Mr. McLellan was appointed by President George Bush as a Presidential Observer to the elections in the People's Republic of Bulgaria. The elections were the first free elections in the country following 45 years of Communist rule. In 1996, he again acted as an observer for the Bulgarian national elections. And again in February, 1999, he acted as an observer for the Nigerian national elections with the International Republican Institute.

Mr. McLellan is a member of the Board of Governors of the Cranbrook Institute of Science, one of Michigan's leading science museums. He helped establish and served for 10 years as president of the Library of Michigan Foundation. He helped establish and served as both President and Chairman of the Michigan Japan Foundation, the private foundation providing funding for the Japan Center for Michigan Universities. He serves on the Board of Directors of the Michigan Information Technology Network.

Mr. McLellan serves as member of the Board of Trustees of Michigan State University-Detroit College of Law.

Mr. McLellan is a former Chairman of the Board of Directors of the Michigan Chamber of Commerce, and is a member of the Board of Directors of the Mackinac Center for Public Policy, the Oxford Foundation and the Cornerstone Foundation.

McLellan is a member of the Board of Directors of the Mercantile & General Life Reassurance Company of America and a Trustee of JNL Trust established by the Jackson National Life Insurance Company. He is also Chairman of the Michigan Competitive Telecommunications Providers Association and in early 2000 was named Chairman of the Information Technology Association of Michigan.

He is a graduate of the Michigan State University Honors College and the University of Michigan Law School. He has served as an adjunct professor of international studies at Michigan State University.

ANTHONY DEREZINSKI

Mr. Derezinski is Vice Chairman of the Michigan Law Revision Commission, a position he has filled since May 1986 following his appointment as a public member of the Commission in January of that year.

Mr. Derezinski is Director of Government Relations for the Michigan Association of School Boards. He also serves as an adjunct professor of law at The University of Michigan Law School and at the Department of Education Administration of Michigan State University, and previously was a visiting professor of law at the Thomas M. Cooley Law School.

He is a graduate of Muskegon Catholic Central High School, Marquette University, the University of Michigan Law School (Juris Doctor degree), and Harvard Law School (Master of Laws degree). He is married and resides in Ann Arbor, Michigan.

Mr. Derezinski is a Democrat and served as State Senator from 1975 to 1978. He was a member of the Board of Regents of Eastern Michigan University for 14 years and currently serves on the Committee of Visitors of the University of Michigan Law School. He also is a member of the Boards of Arbor Hospice and Home Care and the Center for the Education of Women in Ann Arbor.

He served as a Lieutenant in the Judge Advocate General's Corps in the United States Navy from 1968 to 1971 and as a military judge in the Republic of Vietnam. He is a member of the Veterans of Foreign Wars, Derezinski Post 7729, the National Association of College and University Attorneys, the Michigan and National Councils of School Attorneys, and the American Bar Association.

GEORGE E. WARD

Mr. Ward is a public member of the Michigan Law Revision Commission and has served since his appointment in August 1994.

Mr. Ward was the Chief Assistant Prosecuting Attorney in Wayne County in the administration of the Honorable John D. O'Hair. Prior to that, he was a clerk to a justice of the Michigan Supreme Court and in private civil practice for twenty years in the City of Detroit. He recently returned to private practice in Detroit.

He is a graduate of Sts. Peter and Paul High School, Saginaw, the University of Detroit, and the University of Michigan Law School. He is married and the father of five children.

Mr. Ward is an Adjunct Professor of State and Local Government and Franchise Law at the Detroit College of Law at Michigan State University; a member of the Boards of Directors of Wayne Center, Wayne County Catholic Social Services and Wayne County Neighborhood Legal Services; past President of the Incorporated Society of Irish American Lawyers; a former member and President of the Board of Control of Saginaw Valley State University; a former commissioner of the State Bar of Michigan; and a former commissioner and President of the Wayne County Home Rule Charter Commission.

WILLIAM C. WHITBECK

Judge William C. Whitbeck is a public member of the Michigan Law Revision Commission and has served since his appointment in January 2000.

Judge Whitbeck was born on January 17, 1941, in Holland, Michigan, and was raised in Kalamazoo, Michigan. His undergraduate education was at Northwestern University, where he received a McCormack Scholarship in Journalism. He received his LL.B. from the University of Michigan Law School in 1966, and was admitted to the Michigan Bar in 1969.

Judge Whitbeck has held a variety of positions with the state and federal governments, including serving as Administrative Assistant to Governor George Romney from 1966 to 1969, Special Assistant to Secretary George Romney at the U.S. Department of Housing and Urban Development from 1969 to 1970, Area Director of the Detroit Area Office of the U.S. Department of Housing and Urban Development from 1970 to 1973, Director of Policy of the Michigan Public Service Commission from 1973 to 1975 and Counsel to Governor John Engler for Executive Organization/Director of the Office of the State Employer from 1991 to 1993. He served on the Presidential Transition Team of

President-Elect Ronald Reagan in 1980, and as Counsel to the Transition Team of Governor-Elect John Engler in 1990.

In private practice, Judge Whitbeck was a partner in the law firm of McLellan, Schlaybaugh & Whitbeck from 1975 to 1982, a partner in the law firm of Dykema, Gossett, Spencer, Goodnow and Trigg from 1982 to 1987, and a partner in the law firm of Honigman Miller Schwartz and Cohn from 1993 to 1997.

Judge Whitbeck is a member of the State Bar of Michigan, the American Bar Association, the Ingham County Bar Association, the Castle Park Association, and the Michigan Historical Commission and serves as the Chair of the Commission. He is a member of the board of the Michigan Historical Center Foundation and is a Fellow of both the Michigan State Bar Foundation and the American Bar Foundation.

Judge Whitbeck and his wife, Stephanie, reside in downtown Lansing in a 125 year old historic home that they have completely renovated. They are members of St. Mary Cathedral.

Governor John Engler appointed Judge Whitbeck to the Court of Appeals effective October 22, 1997, to a term ending January 1, 1999. Judge Whitbeck was elected in November of 1998 to a term ending January 1, 2005. Chief Judge Richard Bandstra designated Judge Whitbeck as Chief Judge Pro Tem of the Court of Appeals effective January 1, 1999.

BILL BULLARD, JR.

Mr. Bullard is a legislative member of the Michigan Law Revision Commission and has served on the Commission since July 1996.

Mr. Bullard is a Republican State Senator representing the 15th Senatorial District. He was first elected to the Michigan House of Representatives in 1982 and served in that body until his election to the Senate in July 1996. He is currently Chairman of the Senate Transportation and Tourism Committee, as well as the Senate Financial Services Committee. Mr. Bullard also serves as the Vice-Chairman of the Senate Hunting, Fishing and Forestry Committee. He is also the Vice-Chairman of the Senate Finance Committee. Mr. Bullard is also the only practicing attorney serving on the Senate Judiciary Committee.

Mr. Bullard is a graduate of the University of Michigan and the Detroit College of Law. He has three children.

Mr. Bullard is the recipient of the first annual Legislator of the Year award from the Michigan Townships Association. He has been recognized by the National Federation of Independent Business with the Guardian Award, the Oakland County School Board

Association with the Distinguished Service award, the Michigan Soft Drink Association with the Legislator of the Year award. In 1999, he was presented with the State Highway Safety Champion award from the Advocates of Highway and Auto Safety. Mr. Bullard was also recognized by the Michigan Safety Commission in 1999 when they presented him with the State Safety Award. Mr. Bullard was appointed to the Oakland County Business Roundtable, Transportation and Telecommunications Committee by Oakland County Executive L. Brooks Patterson. Mr. Bullard was also recognized for achieving the Michigan Sales Tax Exemption for Rare Coins and Precious Metals by the Industry Council for Tangible Assets. He was also named Legislator of the Year in 2000 by the Michigan Humane Society, as well as by the National Republican Legislators Association.

Mr. Bullard is a member of the National Conference of Commissioners on Uniform State Laws (NCCUSL), National Conference of Insurance Legislators (NCIL), the Fraternal Order of Police of Southwest Oakland County, the Oakland County Bar Association and the State Bar of Michigan.

GARY PETERS

Mr. Peters is a legislative member of the Michigan Law Revision Commission and has served on the Commission since June 1995.

Mr. Peters is a Democrat State Senator representing the 14th Senatorial District. He was elected to the Michigan Senate in November 1994. He serves as the Minority Vice Chair of the Senate Education, Finance, Judiciary, and Natural Resources & Environmental Affairs Committees, and is a member of the Economic Development, International Trade & Regulatory Affairs Committee.

Prior to being in the Legislature, Mr. Peters was Vice President, Investments, for a major national financial services firm. He serves as a Securities Arbitrator for the New York Stock Exchange, National Association of Securities Dealers, and the American Arbitration Association.

Mr. Peters taught Strategic Management and Business Policy at Oakland University, and was an instructor in the Finance & Business Economics Department at Wayne State University. His educational credentials include a B.A. from Alma College (Magna Cum Laude, Phi Beta Kappa), an M.B.A. in Finance from the University of Detroit, and a J.D. from Wayne State University Law School.

His previous government experience includes a term on the Rochester Hills City Council where he served as Chair of the Solid Waste Management Committee, Vice Chair of the Budget & Finance Committee, and a member of the Zoning Board of Appeals and Paint Creek Trailways Commission.

Mr. Peters' community involvement includes serving on the Board of Directors for Common Cause of Michigan, a member of the Environmental Policy Advisory Committee for the Southeast Michigan Council of Governments (SEMCOG) and as Chair of the Air Issues Committee for the Michigan Sierra Club.

Mr. Peters is also a commissioned officer in the U.S. Naval Reserve. He is married and has three children.

JENNIFER M. FAUNCE

Ms. Faunce is a legislative member of the Michigan Law Revision Commission and has served on the Commission since January 1999.

Ms. Faunce is a Republican State Representative representing the 29th House District. She was first elected to the Michigan House in November 1998. She is the Chair of the House Criminal Law and Corrections Committee and a member of the House Regulatory Reform; Senior Health, Security and Retirement; and Tax Policy Committees.

Ms. Faunce was an Assistant County Prosecutor for Macomb County from January 1992 through 1998, as Chief of the Juvenile Court Division.

She holds a Bachelor of Science in Social Science Pre-Law from Michigan State University and a law degree from the University of Detroit School of Law. Ms. Faunce's community involvement includes serving on the Macomb Area Council for Big Brothers/Big Sisters and on the Executive Board for Care House.

LAURA BAIRD

Ms. Baird is a legislative member of the Michigan Law Revision Commission and has served on the Commission since 1997.

Ms. Baird represents Michigan's 70th House District, which consists of East Lansing, Okemos, and part of Haslett, in Ingham County. She was elected to the House of Representatives in November 1994, reelected to a second term in 1996 and a third term in 1998. Ms. Baird serves as democratic chair of the Family and Civil Law Committee, democratic chair of the Criminal Law and Corrections Committee and as a member of the Health Policy Committee.

Ms. Baird grew up in Northern Michigan, where both her father and grandfather served as Probate Judges in adjacent counties. She is an attorney having received her B.S. from Western Michigan University and her law degree, with distinction, from Thomas Cooley

Law School in 1979. Ms. Baird is an alumna of the Bowhay Institute for Legislative Leadership Development and the Flemming Fellows Leadership Institute.

Before her election to the Michigan House of Representatives, Ms. Baird represented Meridian Township's District 11 as an Ingham County Commissioner. As a parent of a son with severe disabilities, she has a long history of volunteering in mental health and disability advocacy organizations. Ms. Baird is past Vice Chair of the Clinton-Eaton-Ingham Community Mental Health Board. Ms. Baird was chosen 1999 Legislator of the Year by The ARC of Michigan; the Michigan Association of Chiefs of Police, 1998 Legislator of the Year; and is the recipient of the 1997 Tell It Like It Is Award from the Alliance for the Mentally Ill of Michigan. The same year she was also chosen Legislator of the Year by the Association for Children's Mental Health.

Ms. Baird is an attorney and has her own private law practice, Baird and Zulakis, P.C., located in Okemos, Michigan since 1980 in partnership with her husband, George Zulakis.

She is a member of the Michigan Sentencing Guidelines Commission and has been appointed as a National Commissioner on Uniform State Laws. In addition, Ms. Baird has served on the Midwest Council of State Governments, Committee on Economic Development and Interstate Competition and the Council of State Governments National Legislative Conference, Corrections and Public Safety Task Force.

DIANNE M. ODROBINA

Since January 1996, Ms. Odrobina, as the Legislative Council Administrator, has served as the ex-officio member of the Michigan Law Revision Commission. The following agencies fall under her supervision: Legislative Service Bureau, Library of Michigan, Legislative Council Facilities Agency, Joint Committee on Administrative Rules staff, Legislative Corrections Ombudsman, Michigan Law Revision Commission, Commission on Uniform State Laws, and the Sentencing Commission. She also serves as a member of the Library of Michigan Board of Trustees and Foundation Board.

Ms. Odrobina has served the Michigan Legislature in several capacities since 1991, serving as the Director of the Senate Majority Policy Office from February 1993 to January 1996. She was previously an Assistant Prosecuting Attorney for Wayne County, attorney for Macomb County Friend of the Court, and in private practice.

Ms. Odrobina holds the degrees of Bachelor of Arts in Political Science from Michigan State University, Master of Business Administration from the University of Detroit, and Juris Doctor from Wayne State University.

KEVIN C. KENNEDY

Mr. Kennedy is the Executive Secretary to the Michigan Law Revision Commission, a position he has filled since December 1995.

Mr. Kennedy joined the faculty of Michigan State University - Detroit College of Law in 1987 and has taught courses in civil procedure, conflict of laws, international trade, and international litigation.

He is a graduate of the University of Michigan, Wayne State University, and Harvard University. He was a law clerk at the U.S. Court of International Trade, was a private practitioner in Hawaii, and served as a trial attorney for the U.S. Department of Justice. He is married.

Mr. Kennedy is the author of nearly forty law review articles concerning international law, international trade, and civil procedure. He is the co-author of World Trade Law, a treatise on international trade law.

GARY GULLIVER

Mr. Gulliver acts as the liaison between the Michigan Law Revision Commission and the Legislative Service Bureau, a responsibility he has had since May 1984.

Mr. Gulliver is currently the Director of Legal Research with the Legislative Service Bureau. He is a graduate of Albion College (with honors) and Wayne State University Law School. He is married and has four children.

Mr. Gulliver is also a Commissioner of the National Conference of Commissioners on Uniform State Laws.