INTRODUCTION
I. CONCEPTUAL UNDERPINNINGS
II. CONSTITUTIONAL PRIVACY LAW
III. TORT LAW
IV. PRIVACY AND DATA PROTECTION STATUTES
V. DATA PROTECTION: VALUES AND STANDARDS
VI. CONTEMPORARY PROBLEMS

Introduction
Privacy concerns in the U.S. date back to the founding era of the nation, as reflected in original Bill of Rights protections for the home, private papers, religion, association and conscience.

The idea of a distinct legal right to privacy originated at the end of the 19th century, when the rise of photography and popular journalism sparked calls for common law privacy rights to protect “inviolate personality” and domestic seclusion.

During the 20th century, legal rights of privacy came to be a significant part of private and public law. Privacy rights emerged in tort law and other state law, constitutional law, and finally, in federal statutes. By the year 2000, reliance upon electronic, computer, surveillance, telephonic, and biometric technologies had prompted calls for aggressive data protection and privacy regulation. Congress and the Federal Trade Commission, along with the private sector, began to heed the call, with the result that lawyers faced a complex array of new privacy law and policy to master. This was especially true for lawyers whose clients are involved in communications, web services, e-commerce, and health and financial services.

The terrorist attacks in New York and Washington D.C. on September 11, 2001 created political pressure to step up “homeland security.” As a consequence, traditional privacies have been downgraded through policies of mandatory information disclosure (by travelers, for example); intergovernmental data-sharing; the USA Patriot Act's heightened criminal law enforcement powers; and secret government monitoring within and without the confines of the Foreign Intelligence Surveillance Act FISA). Privacy is, as some civil libertarians claim, being taken away. But clearly physical and informational privacy is voluntarily surrendered for self-interested and public-spirited reasons all the time.

To better understand these developments, it is useful to review the basics-- the history and values behind privacy
protection in the United States.

I. CONCEPTUAL UNDERPINNINGS

The United States has a uniquely broad body of privacy law. Privacy interests are protected through federal and state constitutional law, through a host of federal and state statutes, and through state common law.

*28 A. The definition of “privacy”

No definition of privacy is universally accepted. Academicians debate the ideal definition of privacy. Clearly, however, privacy relates to the diverse modes by which people, personal information, certain personal property, and personal decision-making can be made less accessible to others. Privacy is protected by law, but also by cultural norms, ethics, and business and professional practices.

B. The definition of the “right to privacy”

Prominent 19th century judges and lawyers popularized one familiar definition of the right to privacy: “the right to be let alone.” A fuller, more contemporary definition of the right to privacy is this one: the claim that society is obligated to adopt laws and promote practices that shield against unwanted intrusion, disclosures, publicity, and interference with matters of personal decision-making, identity and conscience.

C. Types of privacy

There are at least four basic types of privacy. They are (1) informational privacy; (2) physical privacy; (3) decisional privacy; and proprietary.

(1) Employers who read employees' personal email messages without a legitimate business purpose violate expectations of informational privacy. Confidentiality, data protection, data encryption, data security, secrecy, anonymity and adherence to fair information practice standards are informational privacy concerns.

(2) House guests who overstay their welcome result in a loss of physical privacy. Solitude or seclusion can be vital to privacy in a physical or spatial sense. The desire for physical privacy often drives complaints about unlawful search and seizure, peeping toms, trespass, and ‘ambush’ journalism. Bodily integrity, which comes up in discussions of medical care and roadside sobriety testing, is an important, additional physical privacy concern.

(3) Same-sex marriage illustrates a denial by government of decisional privacy. The term “privacy” has come to denote freedom from government interference with personal life. The rights of individuals, married couples, and families to direct their own lives are commonly styled as privacy rights. Disagreements about the proper limits of decisional privacy fuel heated moral debates over gay rights, abortion and physician-assisted suicide.

(4) Identity thieves accessing personal financial data exemplifies a loss of proprietary privacy. Government regulators and the general public characterize identity theft as a privacy problem because it entails seizing otherwise confidential information and personal identifiers. In a related vein, the rights of celebrities and others to control the attributes of their personal identities--their names, voices, trademarks, traits, DNA--are commonly styled as privacy concerns.

D. Why privacy is important

Privacy and privacy rights are highly valued by many in the United States. Why does privacy matter? Some of the traditional answers to this question are that privacy promotes values beneficial individuality, personhood, moral agency, intimate relationships, autonomy, fairness, toleration and limited government.
E. Privacy rights are not absolute

Jurists and scholars who assert that privacy is important uniformly agree that privacy rights are not absolute. Privacy interests cannot always trump all others. No one can have or expect to have all of the privacy he or she may want, even in a free, liberal society based on market principles. Sometimes protecting privacy is simply impractical. It is common for courts to “balance” privacy interests against interests in, inter alia, open government, law enforcement, public health, national security, business, efficiency, and the public's right to know. Courts have held that even where privacy interests are “fundamental,” they can be overcome by “compelling state interests.”

II. CONSTITUTIONAL PRIVACY LAW

A. By virtue of the federal Constitution, Americans have enjoyed federal protection of privacy since the founding of the nation in the late 18th century. The word “privacy” does not appear in the U.S. Constitution. Significantly, however, the Supreme Court has interpreted at least five of the ten original Bill of Rights guarantees and the Fourteenth Amendment as protective of privacy.

(1) The Original Bill of Rights. Furthering family and group privacy, the First Amendment guaranteed freedom of religion and freedom of association. The Third Amendment prohibited military appropriation of private homes. Also protecting the home and its contents, the Fourth Amendment prohibited arbitrary search and seizure of persons and property. The Fifth Amendment prohibited compulsory self-incrimination, allowing for privacy of thought, belief and perspective. The Ninth Amendment reserved unenumerated traditional rights to the people, including rights of bodily integrity, possession and independent decision-making associated with privacy.

(2) The Fourteenth Amendment. After the Civil War, the federal Constitution was amended to reflect the abolition of slavery. The new amendments included the Fourteenth Amendment, which asserted that no state shall deprive a person of life, liberty or property without due process of law. Designed to protect the rights of the newly freed black slaves, the general language of the Fourteenth Amendment has proven to be an important source of protection for substantive liberties sought by private individuals and families. In their written opinions interpreting the Fourteenth Amendment and the Bill of Rights, justices of the Supreme Court have frequently invoked the concept of privacy.

(3) The Reasonable and Legitimate Expectations of Privacy Tests. In the 1960s, the Supreme Court gave the term “privacy” a central role in the interpretation of the Fourth Amendment. Whether at home in bed or in a phone booth, citizens have a right to their “reasonable” and/or “legitimate” expectations of privacy, the Court announced in an important group of cases concerning government search and seizure, the first of which was Katz v. United States, 389 U.S. 347 (1967).

(4) Privacy, Liberty and Substantive Due Process. In the 1960s and 1970s, the Supreme Court also gave the term “privacy” an important role in cases about the regulation of reproduction, sex, marriage and personal information.

(a) In Griswold v. Connecticut, 381 U.S. 479 (1965), the Court held that there is a fundamental right to privacy that prohibits *31 laws criminalizing birth control. In the Griswold decision, the Court argued that privacy has always been an implicit constitutional value, residing in the “penumbra” of the Bill of Rights.

(b) In Loving v. Virginia, 388 U.S. 1 (1967), the Court recognized privacy and equality interests in interracial marriage; and in Stanley v. Georgia, 394 U.S. 557 (1969), it recognized privacy interests in personal use of pornography at home.

(c) Increasingly after Roe v. Wade, 410 U.S. 113 (1973), held that the Fourteenth Amendment is a source of a fundamental right to privacy strong enough to block categorical prohibition of abortion, the Fourteenth Amendment became the major legal tool for persons asserting controversial privacy rights against government.

(d) Whalen v. Roe, 429 U.S. 589 (1977) recognized a Fourteenth Amendment privacy interest requiring confidentiality and security to protect prescription drugs use data collected by the state.

(e) The jurisprudence of constitutional privacy jurisprudence was successfully applied in some landmark “right to die” cases, most notably In Re Quinlan, 355 A.2d 647 (1976). The Court held in Cruzan v,
Missouri Department of Public Health, 497 U.S. 261 (1990) that states may require families, prior to terminating life support, to demonstrate by “clear and convincing” evidence that a family member in a hopeless vegetative state would have wanted to die under those circumstances. The Supreme Court declined in Vacco v. Quill, 521 U.S. 793 (1997), and Washington v. Glucksberg, 521 U.S. 702 (1997), to recognize a right to physician assisted suicide that would invalidate state laws making it a crime for doctors to end the lives of terminally ill patients. On the other hand, the Court declined to strike down Oregon's physician assisted suicide law in Gonzales v. Oregon (2006).

(f) Overruling, Bowers v. Hardwick, 478 U.S. 186 (1986), the Court held in Lawrence v. Texas, 539 U.S. 558 (2003) that the constitution does not to permit states to criminalize adult homosexual sodomy. Lower courts hold that states may criminalize prostitution, sex with minors and incest, consistent with the constitutional right to privacy.

III. TORT LAW

A. Common law doctrines inherited from English common law protected aspects of personal privacy at our nation's inception. For example, the trespass tort deterred physical privacy invasions.

B. Judge Thomas Cooley's A Treatise on the Law of Torts (1880) identified a right of personal immunity described as “a right to be let alone.”

C. In DeMay v. Roberts, 46 Mich.160, 9 N.W. 146 (1881) a Michigan judge declared a right to the privacy of childbirth in the home against a physician who brought an “unprofessional, young, unmarried man” on a house call.

D. As reported in period newspapers, in Manola v. Stevens (1890) a New York judge grants an actress an injunction against publication of an immodest photograph. Innocuous by today's standards, Ms. Manola was photographed wearing tights.

E. In Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890), two Boston lawyers call for the creation of a new legal right to privacy, a right of “inviolable personality.” Inspired by the article, a privacy tort was first recognized by American judges in the early 20th century.

F. In Roberson v. Rochester Folding Box Co. 71 N.Y. 538, 64 N.E. 442 (1902) the New York court decline to create a right to privacy as a remedy for a woman whose photograph was used without her consent in an advertisement.

G. New York Civil Rights Act, Sections 50, 51 (1903) created a right against commercial appropriation of name or likeness, in response to the Roberson case. The law is still in effect today.

*33 H. In Pavesich v. New England Life Ins. Co., 50 S.E. 68 (1905) the tort law privacy right was fully born. No state's supreme court officially recognized the right to privacy until 1905 when the Georgia high court in Pavesich allowed a man to whose photograph was used without his consent in an insurance advertisement to assert a right of privacy.

I. Today the common law of privacy recognizes four basic physical, informational and proprietary privacy rights (but no decisional privacy right as such), first distinguished by William L. Prosser in 48 California L. Rev. 383 (1960). Recognized by the Restatement of Torts (2d) Sections 652B, C, D, E (1964), the four privacy rights are rights against: (1) intrusion upon seclusion, (2) publication of embarrassing private facts, (3) publicity placing a person in a false light, and (4) appropriation of name likeness and identity. The Restatement presentation of the four torts has been adopted by statute or precedent in most states, and has been unaffected by Third Restatement of Torts' innovations in other area of tort law thus far.

J. The scope of the privacy invasion torts. A distinctive feature of the common law privacy torts is that, subject to exceptions for newsworthy publications and First Amendment freedoms, they permit lawsuits against persons
who intentionally and in a highly offensive manner publish or disclose intimate truth. The right to privacy aims to protect persons whose feelings and sensibilities are wounded by having others discover truthful, but embarrassing or intimate matters of fact as a consequence of highly offensive conduct. Courts have generally held that corporations do not have a right to privacy in tort law and have sometimes found that privacy rights do not survive death or are not heritable. The false light privacy invasion requires proof that a falsehood about personal matters has been published. The appropriation privacy tort requires a commercial appropriation of a person's name, likeness or some other indicia of personal identity. Celebrities also pursue a remedy for appropriation under the rubric of the right to publicity.

IV. PRIVACY AND DATA PROTECTION STATUTES

A. Federal Statutes. The federal government began to enact national laws in the 1970s in response to developments in computer, surveillance and other technologies. Some statutes were simply a response to heightened awareness of privacy interests unrelated to technology, such as awareness of privacy interests in traditional school records.

B. Privacy Act and Freedom of Information Act. The United States government holds a vast quantity of personal information gathered in the course of census-taking, tax collection, military management, law enforcement, intelligence gathering, and the administration of health, labor, and human services programs. The Privacy Act of 1974 was enacted in direct response to the increased use by government of computers to collect, store and analyze personal information. Although the Freedom of Information Act opens government records to the public, FOIA works in tandem with the Privacy Act and exempts from disclosure medical, personnel and similar files. Many agency regulations and statutes (the tax code, for example) limit access to personal information held by the federal government.

C. Private-sector records and communications. Personal information is also gathered and stored by the private sector. Privacy law includes comprehensive statutes enacted by Congress, mainly after 1974, governing, for example, the privacy and confidentiality of bank records, school records, video rentals, and telephone calls. This legislation limits access to records and communications, but also regulates the bases for lawful government and other 3rd party accesses. The Family Education and Right to Privacy Act regulates the disclosure of school and university records at institutions receiving federal funding. The most important statute regulating communications is the Electronic Communications Privacy Act (ECPA). It governs, telephone calls, email, and voice mail. Title I of ECPA, commonly known as Title III, regulates government and private wiretapping.


E. Financial Services. Additional major privacy legislation includes Title V of the Financial Services Modernization Act (“Gramm-Leach-Bliley”), which requires that banks, investment companies, insurance companies, and other financial services providers give consumers and customers notice of data-sharing and collection policies and provisions. Consumers and customers may “opt out” of specified information sharing practices among affiliated and non-affiliated businesses. An older federal statute, the Fair Credit Reporting Act, provides the public with protections against certain non-consensual disclosure of nonpublic information found in credit reports, and requires opportunities to correct and contest credit misinformation.

F. Health and HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) regulates access to health information held by physicians, hospitals, insurers, researchers and government. It also sets data security standards for transmission of health information. Health information is protected to an extent in most states under state laws. Although federal regulators entered the arena in the 2000 pursuant to HIPAA, state law was the traditional source of most medical privacy and confidentiality rules. HIPAA only partly preempts state health privacy statutes. Some statutes have specific statutes regulating particular types of information, such as HIV testing data or genetic information.

G. State Statutes. State statutes protect the privacy of many types of communications, including telephone communications that could be recorded or intercepted by police or private investigators. Statutes enacted by lawmakers in the individual fifty states protect the privacy of information contained in many types of business and
professional records. Access to adoption records, criminal histories, and library records is commonly regulated under state law.

V. DATA PROTECTION: VALUES AND STANDARDS

A. Privacy advocates today often call for ethical business practices standards that, since the 1970s have come to be known throughout North America as “fair information practices” standards. Fair Information Practices were recommended by the Report of the U.S. Privacy Protection Commission published in 1977.

B. Under various models of “fair information practices,” standards such as these should be met to the extent possible: (1) the existence of data systems containing personal information should not be a secret; (2) personal information should only be collected for narrow, specific purposes; (3) personal information should only be used in ways that are similar to and consistent with the primary purposes for its collection; (4) personal information should be collected only with the informed consent of the persons about whom the information is collected or their legal representative; (5) personal information should not be shared with third parties without notice or consent; (6) for the sake of accuracy and relevancy, the duration of storage of personal information should be limited; and (7) individuals should have access to personal information about themselves and should be permitted to correct errors; (8) those who collect personal data should insure the security and integrity of personal data and data systems.

C. Internet Privacy Protection Practices and Standards. On May 13, 2000, the New York Times reported that a study of consumer privacy on the Internet financed by the industry and conducted by Prof. Mary Culnan of Georgetown University shows that 65% of commercial Web sites post a privacy warning if they collect personal information, up 14% from the previous year. A spokesperson for the Online Privacy Alliance called the study an “absolute vindication” of self-regulation.

D. TRUSTe is an example of the organizations set up by the firms engaged in electronic commerce industry to certify that companies operating over the World Wide Web pledge to adhere to certain fair information practice standards, such as providing notice to cite users of privacy policies and practices.

E. On May 22, 2000, the Federal Trade Commission (FTC) released its third report on the state of online privacy protection, “Privacy Online: Fair Information Practices in the Electronic Marketplace.” The report called for legislation to protect consumer's online privacy. After the September 11, 2001 attacks, then FTC chairman Timothy Muris announced that the agency would not seek new privacy laws, but would redoubled efforts to enforce existing financial privacy and children's internet laws. The FTC subsequently set up the popular “National Do Not Call Registry” to cut down on marketing telephone calls from persons other than politicians, charities, and businesses with whom consumers have preexisting relationships.

F. European Standards. The “Directive of the European Parliament and the Council of Europe on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data” went into effect in October 1998. It calls for EU member states to enact policies that protect the right to privacy in the processing of personal data. The Directive calls for laws that limit information gathered in the context of commerce to narrowly specified, authorized users and uses. The European Union and the U.S. have negotiated a safe harbor agreement that enables U.S. organizations to comply with EU requirements for adequate privacy protection.

VI. CONTEMPORARY PROBLEMS

Identity theft, spam, pretexting, social security number usage, and data security breaches--these are all on-going information privacy issues. Some major controversies respecting government ‘privacy invasions' in 2006 have included: (1) The GOGGLE controversy. The federal government's ability to require an internet service provider to provide information on the internet surfing/browsing conduct of users deemed relevant to homeland security/law enforcement has been at issue; (2) The FISA Court controversy. The right of the President pursuant to inherent powers or war power authorization to bypass the FISA court and order surveillance of communications of U.S. citizens on U.S. soil was questioned in Congress and in the press; (3) The U.S.A. Patriot Act Controversy. The terms of its reauthorization was an issue closely followed by privacy advocates.
For a run-down of current privacy issues, see EPIC.org, the website of the Electronic Information Privacy Center. Other useful resources are the websites of the American Civil Liberties Union and the Center for Democracy and Technology.

END OF DOCUMENT