PRIVACY AND INFORMATION RIGHTS PART-2

THE INTERNET AND GOVERNMENT INVASIONS OF PRIVACY: E-COMMERCE SURVEILLANCE

Today, the online and mobile behavior, profiles, and transactions of consumers are routinely available to a wide range of government agencies and law enforcement authorities, contributing to rising fears among online consumers, and in some eases, their withdrawal from the online marketplace

LEGAL PROTECTIONS

In the United States, Canada, and Germany, rights to privacy are explicitly granted in, or can be derived from, founding documents such as constitutions, as well as in specific statutes. In England and the United States, there is also protection of privacy in the common law, a body of court decisions involving offences or personal injuries.

Informed consent- consent given with knowledge of all material facts needed to make a rational decision

Opt-in- requires an affirmative action by the consumer to allow collection and use of consumer information

Opt-out- the default is to collect information unless the consumer takes an affirmative action to prevent the collection of data

The Federal Trade Commission's Fair Information Practices Principles

Notice/Awareness (core principle)	Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/ inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of the data.
Choice/Consent (core principle)	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties. Opt-in/opt-out must be available.
Access/Participation	Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security	Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement	There must be a mechanism to enforce FIP principles in place. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulation.

The European Data Protection Directive

In Europe, privacy protection is much stronger than it is in the United States. In the United States, private organizations and businesses are permitted to use PII gathered in commercial transactions for other business purposes without the prior consent of the consumer (so-called secondary uses of PII). In the United States, there is no federal agency charged with enforcing privacy laws. Instead, privacy laws are enforced largely through self-regulation by businesses, and by individuals who must sue agencies or companies in court to recover damages. This is expensive and rarely done. The European approach to privacy protection is more comprehensive and regulatory in nature. European countries do not allow business firms to use PII without the prior consent of consumers. They enforce their privacy laws by creating data protection agencies to pursue complaints brought by citizens and actively enforce privacy laws.

Safe harbor- a private self-regulating policy and enforcement mechanism that meets the objectives of government regulators and legislation but does not involve government regulation or enforcement.

PRIVATE INDUSTRY SELF-REGULATION

The online industry in the United States has historically opposed online privacy legislation, arguing that industry can do a better job of protecting privacy than government. However, individual firms such as Facebook, Apple, Yahoo, and Google have adopted policies on their own in an effort to address the concerns of the public about personal privacy on the Internet. The online industry formed the Online Privacy Alliance (OPA) in 1998 to encourage self-regulation in part as a reaction to growing public concerns and the threat of legislation being proposed by FTC and privacy advocacy groups.

PRIVACY ADVOCACY GROUPS

There are a number of privacy advocacy groups on the Web that monitor developments in privacy

Epic.org (Electronic Privacy Information Center)	Washington-based watch-dog group
Privacyinternational.org	Watch-dog organization focused on privacy intrusions by government and businesses
Cdt.org (Center for Democracy and Technology)	Foundation- and business-supported group with a legislative focus
Privacy.org	Clearinghouse sponsored by EPIC and Privacy International
Privacyrights.org	Educational clearinghouse
Privacyalliance.org	Industry-supported clearinghouse

THE EMERGING PRIVACY PROTECTION BUSINESS

As Web sites become more invasive and aggressive in their use of personal information, and as public concern grows, a number of firms have sprung up to sell products that they claim will help people protect their privacy. Venture capital firms have picked up the scent and are investing millions in small start-up companies based on the premise that people will pay to protect their reputations.

TECHNOLOGICAL SOLUTIONS

A number of privacy-enhancing technologies have been developed for protecting user privacy during interactions with Web sites such as spyware blockers, pop-up blockers, cookie managers, and secure e-mail. However, the most powerful tools for protecting privacy need to be built into browsers.

Microsoft, Mozilla, Google, and Apple have all introduced a default Do Not Track capability. Microsoft ships its browser with the default set to "Do Not Track."