A. Laws and Regulations

1) What laws apply to protection of privacy issues in your legal system? Are there civil code/legislative/common law provisions that protect individuals against privacy violations regarding:

a) In the Public Sector
   • Access by individuals to information collected by various government agencies about them?
   • Protection from disclosure of that information to third parties?
   • Access by the media or members of the public to government records, for example, those regarding government decision-making and action, and limitations put on that access?
   • Limitations put on information sharing between government agencies?

b) In the Private Sector
   • Protection from disclosure to third parties of personal information collected in the world of e-commerce, for example
     • personal information provided through the use of credit/debit cards and other electronic transfers of funds
     • personal information in relation to credit reporting and banking transactions
     • records of a customer’s usage (telephone; online activity)
     • records kept for insurance coverage and other social services benefits provided by the private sector?
     • Protection from surreptitious collection of information via the Internet, for example, through Internet electronic surveillance technologies such as “spyware” or “adware”?

The United States uses a sectoral approach to privacy laws that relies on a mix of legislation, regulations, self-regulation, and civil and criminal enforcement. The United States Constitution does not specifically provide for a fundamental right to privacy. The Fourth Amendment to the United States Constitution offers strong privacy protections for our homes in
the physical world. Absent special circumstances, the government must obtain a search warrant based on probable cause before searching a home for evidence of crime. While the Constitution itself does not explicitly create an individual right of privacy, the Supreme Court’s interpretation of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments has created constitutional protection for personal privacy rights. In addition to privacy protection through the United States’ constitution and federal common law, the several States also have created their own rights of privacy, either explicitly in their state constitutions, through state legislative enactments, or through state common law providing for torts associated with the violation of various privacy rights.

Congress also has responded to concerns about privacy by enacting many statutes which regulate the government’s use of private information. For example, the Privacy Act of 1974, which applies only to records of personal information held by federal agencies, prohibits the disclosure of records without the written request of the individual to whom the record pertains and seeks to protect personal privacy by regulating the government’s use, exchange, and dissemination of records concerning private individuals. The Act provides twelve disclosure exemptions to this prohibition. If information falls within one of the exemptions, it can be disclosed and otherwise shared without the individual’s permission. For example, an agency need not obtain an individual’s consent before disclosing the content of his records if such disclosure is within the agency, for routine use, or for disclosure to law enforcement.

Congress also enacted the Financial Privacy Act, which helped fill gaps in the Privacy Act. The Financial Privacy Act governs information flows between the government and private financial institutions. The statute prohibits banks from supplying the government with personal financial information except in three specific cases: (1) where the customer consents to the information transfer; (2) where the government has a valid subpoena or search warrant for the records; or (3) where the government submits a formal written request under special circumstances. The Financial Privacy Act further sets forth the procedure by which a bank customer may challenge a government request, authorizing the individual to move a court to quash an administrative summons or judicial subpoena, or to obtain an injunction against a formal request. The Financial Privacy Act also mandates strict procedural requirements for the inter-agency exchange of financial records already legitimately in the possession of a government
agency. The Act prohibits the transfer of financial records between federal agencies unless the
government can demonstrate that the receiving agency has a legitimate law enforcement inquiry,
within its jurisdiction, pertaining to the requested records.

Another major federal statute regulating information within the government’s possession
is the Freedom of Information Act (FOIA), which was enacted to require the federal government,
including agencies, to provide access to its records. The FOIA is mainly a disclosure statute. The
Privacy Act explicitly exempts from its non-disclosure requirements records for which the FOIA
mandates disclosure. Under the FOIA, any individual, regardless of country of residence, has the
right to request access to federal agency records or information unless protected from disclosure
pursuant to an exemption or exclusion. Exemptions include information that is authorized to be
kept secret in the interest of national defense or foreign policy, trade secrets, commercial or
financial information, personnel files, medical files, information compiled by law enforcement,
and information that would lessen the ability of the government to obtain necessary information
in the future.

In addition to statutes aimed at the governmental collection, use, and disclosure of
information, Congress has enacted statutes aimed at protecting private information held by non-
governmental entities. For example, the Health Insurance Portability and Accountability Act of
1996, regulates how certain entities may use and disclose individually identifiable health
information. The Act increases patient control over the accuracy and disclosure of their health
information, and includes civil and criminal penalties for violators. The Gramm-Leach-Bliley
Act includes provisions to protect consumers’ personal financial information held by financial
institutions.

Congress also has acted to protect from the surreptitious collection of information through
the Internet through legislation such as the Computer Fraud and Abuse Act (CFAA), the
Electronic Communication Privacy Act (ECPA), the Stored Wire and Electronic Communications
and Transactional Records Act (SCA), and the Wiretap Act. The CFAA is triggered when
someone accesses a computer used in or affecting interstate commerce without authorization or
when a person exceeds authorized access. The CFAA includes a private cause of action for its
violation.

The ECPA prohibits intentional unauthorized access to a facility through which an
electronic information service is provided or intentionally exceeding an authorization to access that facility and obtaining access to an electronic communication while it is in electronic storage. The ECPA applies to both government employees and private citizens. It protects communications in storage as well as in transit. Live telephone communications, voice mail messages, email messages, text messages, and instant messages are all forms of wire and electronic communications that are protected by the ECPA. Unless the interception or unauthorized access of a wire, oral, or electronic communication is covered by one of several statutory exceptions or defenses, violation of the ECPA is both a civil violation and a federal crime.

The SCA creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private information. The SCA limits the government’s ability to compel providers to disclose information in their possession about their customers and subscribers. The SCA also places limits on the ability of Internet Service Providers to voluntarily disclose information about their customers and subscribers to the government. The federal Wiretap Act protects the privacy of wire, oral, and electronic communications. The Wiretap Act’s purposes are (1) protecting the privacy of wire and oral communications; and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.

Congress also has acted to protect privacy in areas such as video rental history, telemarketing practices, and debt collection practices. For example, the Video Privacy Protection Act forbids a video rental or sales outlet from disclosing information concerning what tapes a person borrows and buys, or releasing other personally identifiable information without the informed, written consent of the customer. The Video Privacy Act allows consumers to sue for damages if they are harmed by violations of the Act. The Telephone Consumer Protection Act was adopted to address certain telemarketing practices that may invade consumer privacy. In addition to federal agency and state government enforcement actions, the Act authorizes consumers to sue violators for the greater of $500 for each violation or actual damages, with the possibility of recovering treble damages.

Most of the several States also have enacted statutes that prohibit unauthorized access to
computers. Several States have statutes that prohibit an authorized user from exceeding the granted authority to access a computer or computerized information. Most states also have enacted various laws to protect private information, and recognize a host of privacy rights through their common law. For example, businesses who make certain promises regarding their privacy policies may face lawsuits for deceptive trade practices if they do not live up to their promises.

2) **What laws apply with respect to the investigation and enforcement of privacy rights?**

- How strong is the protection?
- Are the laws binding or advisory?
- How does an individual make a complaint when a private actor or government breaks privacy laws?
- Who prosecutes or enforces -- for example, a privacy commissioner, administrative body, such as a privacy tribunal?
- Is there a right to a court remedy?
- Are there out-of-court dispute resolution options?

Privacy statutes are enforced through private litigation if the particular statute provides for an individual cause of action and through criminal prosecution if the particular statute provides for criminal penalties. For example, the Privacy Act authorizes the award of civil remedies to individuals when an agency violates the Act. The Privacy Act includes remedies such as requiring an offending agency to amend incomplete or inaccurate records, enjoining disclosure, ordering production of improperly withheld records, awarding actual damages sustained by the individual as a result of the agency violation, and awarding costs of prosecution in successful actions against the agency. The Financial Privacy Act creates civil penalties against the government for violation of its provisions. Permissible damages include any actual damages suffered by the bank customer, any costs or fees incurred in a successful action against the government, and punitive damages when the violation is proved willful or intentional. The Privacy Act makes it a misdemeanor to knowingly and willfully disclose agency records in
violation of the Act. Violators of the Health Insurance Portability and Accountability Act may face criminal penalties of up to ten years and fines up to $250,000. Aggrieved individuals also may have the right to sue for common law torts for the violation of certain privacy rights.

Additionally, some statutes authorize federal agency enforcement through agencies such as the Federal Trade Commission and the Federal Communications Commission. The Privacy Act also established the Privacy Protection Study Commission to monitor and report on the Privacy Act’s effectiveness in preserving personal privacy.

B. Private-Sector Initiatives

1) Do particular companies, industries or professional associations in your country govern themselves regarding the protection of privacy? For example, are there privacy policies, professional codes, voluntary industry standards?

2) Who or what body, if any, ensures that these standards are met?

The law of contracts is an important way that privacy is protected in the commercial context. The parties to a contract are free to decide the privacy levels that are suitable for themselves, and may include explicit contract terms to protect information. Businesses naturally prefer voluntary arrangements such as codes, standards, and privacy seal programs rather than laws, as they afford more control and flexibility. For example, private companies, known as seal organizations, have established means of certifying whether other companies have privacy policies and are complying with their stated privacy policies. These seal organizations provide websites with a cost-effective means for building consumer confidence in the privacy of their information. There are several prominent seal organizations, including BBBOnline, Truste, CPA webtrust, Privacy Seal, SAFECertified, and Enonymous.com. Typically, the client website
provides the seal organization with a description of the information the website will gather, the
uses to which it will be put, the parties with whom it will be shared, the choices that will be
afforded consumers regarding collection use and disclosure, and the applicable security. The seal
organization then reviews the client site to determine whether it complies with the client’s privacy
statement.

The seal organization thereafter monitors the client site to determine continued
compliance. When the seal organization is satisfied, the site is awarded the seal, which is then
displayed on the website. When the user clicks on a genuine seal, it activates a hyperlink to the
seal organization’s website, to prove that the seal is genuine. Once the seal is posted, consumers
may lodge privacy complaints with the seal organization, which then engages in dispute
resolution. Where the seal organization determines that the client violated its privacy policy, the
seal organization investigates. If the seal organization concludes that the site is not compliant, it
assists the client in coming into compliance. Where the client is not cooperative, remedies
include revocation of the seal, and in aggravated cases, communication to an appropriate
governmental agency. However, the seal organization is not in a position to obtain damages for
any injured user of the site.

Because consumers value their privacy, market pressure is a powerful force in
encouraging companies to develop and enforce adequate privacy and security policies and
mechanisms. For example, the popular social networking website Facebook recently has
experienced negative consumer backlash over its privacy policies, with consumers contending
Facebook has been selling information that users thought was private.

C. International and Cross Border Issues
1. How is privacy protected when information is exchanged or transferred to other countries?

2. Are there any agreements, laws or international treaties or protocols, to protect privacy issues in this situation?

3. Does your country limit its exchange of information to countries with similar protections of privacy?

Though not having the force of law in the United States, the privacy guidelines issued by the Organization for Economic Cooperation and Development (OECD) in 1980 are an important part of privacy enforcement. The OECD consists of representatives from 29 countries, including the United States, that work to coordinate policies with the aim of fostering international trade.

The European Commission’s Directive prohibits the transfer of personal data to non-European Union nations that do not meet the European “adequacy” standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. In comparison to the European Union, the United States offers less privacy rights to individuals and the disclosure of their information. To bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce, in consultation with the European Commission, developed the Safe Harbor Principles which allow individual companies to implement procedures deemed adequate for receipt of data from the European Union. Safe Harbor is not available, however, to banks because of the Gramm-Leach-Bliley Act.

The United States’ privacy laws generally do not prohibit private information sharing with entities in foreign countries as a specific topic of regulation. However, the United States’ privacy laws will apply to the person or entity in the United States, and thus that person or entity has the incentive to ensure that any information it shares which is covered by one of the privacy statutes, or by common law, is adequately protected. For example, if a company located within the United States outsourced its data processing of consumer information to a company in a foreign location which had weaker privacy laws, the company located in the United States still would be subject to applicable civil and criminal enforcement in the United States. It therefore has incentive to
ensure its vendors comply with any applicable privacy laws and security requirements.