

Exam Number: _____

GEORGETOWN UNIVERSITY LAW CENTER
EXAMINATION
"THE LAW OF INFORMATION PRIVACY"
(3 HOURS)

Professor Rotenberg

May 8, 2000

INSTRUCTIONS:

1. This is an OPEN book examination.
2. You should select three of the following four questions. Each question will receive equal weight. There will be no additional credit for answering a fourth question.
3. Use only one side of the paper. Write clearly.
4. I will consider only the material that is in the exam book or in the typed submission.
5. Organize your answers carefully. Note the particular format requested in each question.

This exam consists of 8 pages including this cover page. Please be sure that your exam is complete.

PLEASE DO NOT TURN THE PAGE UNTIL THE PROCTOR GIVES THE SIGNAL

GEORGETOWN UNIVERSITY LAW CENTER
EXAMINATION
"THE LAW OF INFORMATION PRIVACY"
(3 HOURS)

Professor Rotenberg

May 8, 2000

Question 1

You are counsel to the Senate Judiciary Committee.

The Internet Crime Prevention Act was recently introduced in Committee. It is intended to strengthen computer crime laws by increasing criminal penalties and making it more difficult for people who commit computer crime to escape detection. One provision of the bill states the following:

USER ACCOUNTABILITY – Users of Internet services who send email shall be required to include their actual name in the email header or, if they do not include their actual name, such users shall be required to provide contact information for an Internet Service Provider who will, upon request, disclose the actual identity of the user to any person who so requests.

Draft a brief memo for the Committee Chairman on whether such a measure would be Constitutional.

Question 2

You are counsel to the Article 29 Working Party, established by the EU Data Directive

The Chairman of the Working Party has asked you to review the privacy provisions contained in the Cable Communications Policy Act of 1984 to determine whether US companies offering interactive video services to European consumers will be in compliance with Article 25 of the EU Data Directive

Draft a brief memo for the Chairman.

Question 3

You are counsel to KewlVentures, a new hi-tech start-up that plans to offer a wide range of online services, including book and CD sales, investment advisory services, news and health information.

The CEO of KewlVentures indicates that she wants her company to be a “privacy leader.” She says that profitability is of course important, but she also believes her company can do “the right thing on privacy.” She is prepared to consider a wide range of policy, technical, and legal measures to address the public’s concern about privacy.

Write a brief memo for the CEO that outlines five steps you think the firm could take to address privacy concerns.

Question 4

If Brandeis and Warren were to revisit their article on the Right of Privacy today, what would they say? Cite specific cases, statutes, and developments in business practices and technology where appropriate.

END OF EXAM

WRITE NOTHING AFTER TIME IS CALLED

CABLE COMMUNICATIONS POLICY ACT (1984)

[Public Law 98-549]

47 U.S.C. § 551. Protection of subscriber privacy

(a) Notice to subscriber regarding personally identifiable information; definitions

(1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of -

(A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;

(B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

(C) the period during which such information will be maintained by the cable operator;

(D) the times and place at which the subscriber may have access to such information in accordance with subsection (d) of this section; and

(E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

(2) For purposes of this section, other than subsection (h) of this section -

(A) the term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons;

(B) the term "other service" includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and

(C) the term "cable operator" includes, in addition to persons within the definition of cable operator in section 522 of this title, any person who

(i) is owned or controlled by, or under common ownership or control with, a cable operator, and

(ii) provides any wire or radio communications service.

(b) Collection of personally identifiable information using cable system

(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

(2) A cable operator may use the cable system to collect such information in order to -

(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or

(B) detect unauthorized reception of cable communications.

(c) Disclosure of personally identifiable information

- (1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.
- (2) A cable operator may disclose such information if the disclosure is -
- (A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;
 - (B) subject to subsection (h) of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; or
 - (C) a disclosure of the names and addresses of subscribers to any cable service or other service, if -
 - (i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and
 - (ii) the disclosure does not reveal, directly or indirectly, the -
 - (I) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or
 - (II) the nature of any transaction made by the subscriber over the cable system of the cable operator.
- (d) Subscriber access to information A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.
- (e) Destruction of information A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) of this section or pursuant to a court order.
- (f) Civil action in United States district court; damages; attorney's fees and costs; nonexclusive nature of remedy
- (1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.
 - (2) The court may award -
 - (A) actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;
 - (B) punitive damages; and
 - (C) reasonable attorneys' fees and other litigation costs reasonably incurred.
 - (3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.
- (g) Regulation by States or franchising authorities Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.
- (h) Disclosure of information to governmental entity pursuant to court order A governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order -

(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

EUROPEAN UNION DATA PROTECTION DIRECTIVE (1995)

Article 25 Principles

1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.
3. Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article Member States shall take the measures necessary to prevent the transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:
 - 1) the data subject has given his consent unambiguously to the proposed transfer, or
 - 2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request, or
 - 3) the transfer is necessary for the conclusion or for the performance of a contract concluded in the interest of the data subject between the controller and a third party, or
 - 4) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
 - 5) the transfer is necessary in order to protect the vital interests of the data subject, or
 - 6) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in

general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such guarantees may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations granted pursuant to paragraph 2. If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2). Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient guarantees required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.