FTC Privacy Panel – Security 1 Working Group – Preliminary Outline of Issues

(February 18, 2000)

I. Introduction

- A. What sort of world do we want?
- B. How far can this part of the exercise go toward reaching that goal?

II. Computer Security and Security Standards

- A. Background
- B. "Threats"
- C. "Attacks"
  - i. Passive attacks
    - a. eavesdropping (loss of confidentiality)
    - b. traffic analysis (loss of privacy)
  - ii. Active attacks
    - a. message modification (loss of integrity)
    - b. denial of service (loss of communication)
    - c. impostoring (loss of identification)
  - iii. Security services
    - a. authentication (who are you?)
    - b. authorization (what can you do?)
    - c. accountability (what did you do?)
  - iv. Other concepts
    - a. non-repudiation
    - b. containment

B. Security Standards

i. General discussion

a. The wonderful thing about standards is that there are so many to choose from.

b. May be based more on functionality than on policy?

ii. Specific standards used in industry

a. International Standard Organization, Geneva, ISO 7498-2-1988(E), Information Processing Systems OSI Basic Reference Model – Part 2: Security Architecture

b. BS7799: A Code of Practice for Information Security Management published by the British Standards Institution in the UK

c. Certificate Practices Statements (CPSs)

d. Financial audit standards

e. Others

iii. Seal programs

a. TRUSTe

b. BBBOnline

(1) Reliability seal program

(2) Privacy seal program

(3) Web Trust (AICPA)

c. PricewaterhouseCoopers

C. Who Currently Develops and Sets Security Standards?

i. Single company scope

ii. Trade group scope

iii. Even broader scope

D. Sources for Standards

i. Common Criteria for Information Technology Security Evaluation (see http://csrc.nist.gov/cc/ccv20/ccv2list.htm)

ii. National Research Council study, “Trust in Cyberspace”

III. Privacy and Security – Legal Provisions

A. The Children's Online Privacy Protection Act (COPPA) and its accompanying regulations require "reasonable procedures to protect the . . . security . . . of personal information collected from children." 16 C.F.R. 312.8.

B. The privacy section of the Gramm-Leach-Bliley Financial Services Act of 1999 states that "each financial institution has a continuing obligation to . . . protect the security and confidentiality of those customers' non-public personal information." The Act’s implementing agencies have signaled that security standards could be in the works in the near future. [Note: proposed rules have recently released by Federal Reserve, Comptroller of the Currency, and Department of the Treasury]

C. Digital Millennium Copyright Act (DMCA/ Public Law No: 105-304)
Under the DMCA, a person can be subject to both criminal and civil penalties for circumventing a copy control technology that protects copyrighted works. If personal data is a copyrighted database, there is some arguable privacy protection here.

D. 18 USC § 1030 – Fraud and related activity in connection to computers. In general, provides criminal penalties for intentionally accessing a computer without authorization.

E. HIPPA/HHS regulations re: protection of patient medical data held in electronic form

F. Other existing legislation

IV. Other Relevant Legal Provisions Relating to Security

A. DOD computer security standards

B. NIST FIPS

C. FBI/NIPC

D. OCC/Fed/SEC procedures or lack thereof

E. Other possible legal standards (*e.g.*, simple negligence, class actions, etc.)

V. Defining Terms

A. "Security and confidentiality"

B. "Integrity of records"

i. Is this term used more in a technical (preventing forgery) sense?

ii. Or legal (completeness and accuracy) sense?

C. "Unauthorized access or use"

i. Is this term used more in a technical (aimed at outside hackers) or legal (aimed at insiders exceeding authority) sense?

ii. Who defines authority?

iii. Disclosure to third parties?

VI. Regulating Security – The "Sliding Scale" Problem

A. Security is inherently contextual. Adequate security for one context and for one class of data is not necessarily adequate for a different context or another class of data.

i. Principles of risk management, cost-benefit analysis of security measures

ii. Security is a "means" while privacy is an "end."

B. Can we rely on data holders to determine appropriate security levels?

i. The data has value to them (but loss of control may mean more to the subject).

ii. They will spend an amount on security that reflects that value (see risk management).

C. What about market failures?

i. Sometimes security of particular personal data is more valuable to the customer than to the data holder.

ii. Are these circumstances frequent? Predictable? Sufficiently serious to require that some outsider set minimum security standards?

iii. Never underestimate the lure of convenience.

VII. Issues that Arise If One Concludes that Market Failures Justify Imposing Security Standards:

A. Are there particular classes of data that require standardized protection?

i. Or, put another way, are there classes of data that do not require standardized protection?

ii. Which is the default case – "protected" or "defenseless"?

B. How can data holders identify such classes of data?

C. What about small businesses? Should a site earning $500 a month in credit card purchases spend as much to protect card numbers as a site earning $500,000 a month?

VIII. What Are the Costs of Imposing Security Standards?

A. Costs to data holders?

i. Financial?

ii. Other? (*e.g.*, access difficulties)

B. Costs to the consumer?

i. Financial?

ii. Other? (*e.g.*, can the state trooper at the accident scene access my medical records immediately?)

C. Costs to Society?

i. Delayed technology (DoD experience)

ii. Other

IX. Benefits of Imposing Security Standards

A. To consumer

i. Builds consumer confidence in e-commerce

ii. Other

B. To data holders

i. Increased market for e-commerce and services

ii. Other

C. To society

X. Pending Legislation

A. H.R. 313

B. H.R. 2413

C. H.R. 2882

D. S. 809

E. S. 854

F. S. 1993

G. S. 2063

XI. Conclusions and Recommendations