Legal Issues in E-Commerce Testing: Meeting Privacy Requirements

James B. Speer, Jr., Ph.D., J.D.

Senior Process Specialist

Data Dimensions, Inc.

Related Work

"Legal Issues in eCommerce Testing," Software Testing Analysis and Review Conference [STAR West 1999], San Jose, California

"Outsourcing Software Testing: Back Office Challenges in eCommerce Transactional Analysis," presentation for Hewlett-Packard, AIO Division, San Diego, California

"Complex Algorithms in Data Mining: Software Testing Models and Data Integrity Standards," prepared for American Electronics Association, Manufacturing Committee, and Hewlett-Packard, La Jolla, California

Related Work

"Legal Issues Relevant to eCommerce Site Development," White Paper for Enterprise Services Division (Redmond, WA: Microsoft, 2000)

http://www.microsoft.com/technet/ecommerce/legalreq.asp

"Electronic Commerce Testing: Emergence of Legal Standards," presentation to Software Testing and Analysis and Review conference [STAR East 2000], Orlando, Florida

Related Work

"The Impact of New Privacy Protection Standards on Secured Online Transactions," presentation to Digital Insight, Los Angeles, California

"Legal Dynamics in Business-to-Business Transactions: Quality Assurance Standards for Electronic Commerce," presentation for Hewlett-Packard, Boise, Idaho

"Legal Issues in E-Commerce Testing: Emerging Requirements and Practical Guides," presentation for Hewlett-Packard World Forum 2000, Philadelphia, Pennsylvania

Reference Materials

UNITED STATES LAW

FAIR CREDIT REPORTING ACT (1970)
PRIVACY ACT (1974)
FREEDOM OF INFORMATION ACT (1974)
FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (1974)
RIGHT TO FINANCIAL PRIVACY ACT (1978)
PRIVACY PROTECTION ACT (1980)
CABLE COMMUNICATIONS POLICY ACT (1984)
ELECTRONIC COMMUNICATIONS PRIVACY ACT (1986)
VIDEO PRIVACY PROTECTION ACT (1988)
EMPLOYEE POLYGRAPH PROTECTION ACT (1988)
TELEPHONE CONSUMER PROTECTION ACT (1991)

Reference Materials

UNITED STATES LAW ,Cont.

DRIVER'S PRIVACY PROTECTION ACT (1994)
TELECOMMUNICATIONS ACT (1996)
CHILDREN'S ON-LINE PRIVACY PROTECTION ACT (1999)
FINANCIAL SERVICE MODERNIZATION ACT (1999)
FEDERAL TRADE COMMISSION ACT (2000)

Reference Materials

INTERNATIONAL PRIVACY LAW

UNIVERSAL DECLARATION OF HUMAN RIGHTS (1948)
COUNCIIL OF EUROPE CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS (1950)
OECD PRIVACY GUIDELINES (1980)
COUNCIL OF EUROPE CONVENTION ON PRIVACY (1981)
UN GUIDELINES FOR THE REGULATION OF COMPUTERIZED PERSONAL FILES (1990)
EUROPEAN UNION DATA PROTECTION DIRECTIVE (1995)
EUROPEAN UNION DIRECTIVE FOR THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR (1997)

Reference Materials

INTERNATIONAL PRIVACY LAW ,Cont.

OECD CRYPTOGRAPHY GUIDELINES (1997)
ITALIAN DATA PROTECTION ACT (1996)
GUIDELINES FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE COLLECTION AND PROCESSING OF PERSONAL DATA ON INFORMATION HIGHWAYS (COE 1999)
LAW FOR THE PROTECTION OF PRIVATE LIFE IN CHILE (1999)
THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (CANADA 2000)
REGULATION OF INVESTIGATORY POWERS ACT (2000)

Privacy Organizations

Harvard Information Infrastructure Project
Electronic Privacy Information Center (EPIC)
National Association of Attorneys General
Center for Democracy and Technology
Cyberspace Law Center, Privacy Resources
Privacy Archives
Internet Free Expression Alliance
Internet Privacy Coalition
The Privacy Forum
Privacy and Information Access
Privacy International
Privacy Rights Clearinghouse

The Privacy Context

E-Commerce Categories

- Information Access
- Self Services
- Shopping Services
- Interpersonal Communication
- Virtual Enterprises

E-Commerce Steps of Production

- Attraction of Customers
- Content on Goods and Services
- Customization to Customer Preferences
- Closing the Deal and Payment
- Customer Support, Fulfillment, Delivery
- Data Mining

The E-Commerce Landscape

"User Beware"

- Percent of all cases of credit card fraud attributable to electronic commerce: 50%

- Number of cases of "Identity Theft" reported to major credit bureaus each day: 1,500

The E-Commerce Landscape

“User Beware”

Visitors who refuse to give information because they think it is too personal or worry about how it might be misused

- Financial 64 %
- Retail 59 %
- Insurance 56 %
- Health sites 44 %

Qualitative Crossroads

The transition from concerns of functionality and robustness to security and confidentiality are requiring

(a) an awareness of and sensitivity to legal issues

(b) the incorporation of legal standards into test planning.

E-Commerce Testing

- Traditional (Functional)
  - Usability
  - Performance
  - Reliability
- Today (Risk-Sensitive)
  - Legal Standards
  - External Requirements
  - Business Rules

Testing Priorities

- Identify and assess all critical business functions
- Ensure Internet connectivity
- Secure online transactions
- **Conduct privacy audit**
- Conduct vulnerability analysis
- Prioritize recovery requirements
- Reinforce disaster avoidance measures

Confidentiality Concerns

- Health sites may track clinical data (test results from cancer or HIV exams) or genetic markers
- Children's sites may collect names, ages and toy preferences
- E-tailers may collect credit card, social security and banking numbers, along with personal profiles and analyses of online behavior

Emerging Privacy Parameters

- Medical Privacy and New Consent Regulations (HIPAA)
- Data Privacy and Financial Services Requirements (FCRA and Gramm-Leach-Bliley)
- Proposed Comprehensive Online Consumer Privacy Standards
- Workplace surveillance
- Cooperation with law enforcement

Testing Online Consumer Privacy

Privacy concerns are particularly important to accommodate in light of

(a) new federal and state requirements

(b) emerging international and industry standards

(c) more stringent business rules.

Enhancing Privacy Protections

Incorporating Legal Standards in Testing Will Promote Best Practices by

(a) clarifying business rules and policies

(b) encouraging compliance-checking in static and dynamic tests, and

(c) helping differentiate corporate interests and consumer protection.

Vexing Privacy Issues

- Encryption and limits on technological solutions
- Roles of Chief Privacy Officers
- Privacy “seals of approval” and limits on self-policing
- Requirements for special populations, filtering software
- Customer lists of “dot-gones” in bankruptcy proceedings

Privacy Policy Basics

From Web Sites Consumers Receive

- notice of the personal identifying information collected and its uses;
- choices about how their information is used;
- access to their own information and the ability to correct errors; and
- adequate security to protect the information collected.

Policy Compliance Criteria

- Database management systems that can delete consumers wanting to opt-out.
- Authentication systems to ensure that people requesting access to information gathered about them are entitled to the information.
- Systems that allow authenticated people to view the information gathered about them and make changes to it.
- Auditing systems that track access to consumer information and changes made.

Opt-Out Notices

- Must be labeled appropriately, placed on frequently accessed Web pages, such as ones where transactions are completed.
- Must include text or visual clues to encourage users to scroll down in order to view the entire notice.
- Must be free of other elements, such as graphics or audio components, that could distract attention from the text of the notice itself.

Framing Legal Issues

- Quality Criteria
- External Requirements
- Risk Management
- Domain of "The Bad Man" in FTC Consent Orders

Tracking the Underlying Commercial Issues

- Concerns about **What** is being sold
- Concerns about **How** the goods or services are being sold
- Concerns about **Buyers** and **Target Markets**
- Following the **money**

Test Planning for Privacy Issues

- Specifically Requested Information
- Clickstream Data
  - Navigational Information
  - Transactional Details
- Public Communications
- Private Content

Fashioning Privacy Test Cases

- Cookies
- IP Address
- Referers
- GUID
- Security Threats
  - Keystroke monitoring
  - Malicious scripts and applets
  - Server attacks, unauthorized access

Meeting the Social and Legal Challenges

Conclusion