
Chapter XI

Liability for System and Data Quality

Robert D. Sprague
Eastern New Mexico University, USA

ABSTRACT

This chapter discusses various theories of legal liability related to computer system and data quality. Contract-based theories are discussed in detail, as most computer systems are acquired and data are accessed through some form of contractual relationship. Additional tort-based theories of liability are also discussed, particularly relating to publication of inaccurate data. As presented in this chapter, purchasers of defective computer hardware or software and users of inaccurate data have very limited legal remedies available. Further, the legal remedies that may be available are typically severely restricted by the contract through which the computer system is acquired or the data are accessed.

INTRODUCTION

Accompanying the proliferation of computers in almost every facet of life is an underlying risk to financial and physical well-being related to computer system and data quality. Software errors have been directly linked to business

disruptions, loss of services (such as metropolitan telephone services), plane crashes, and even deaths (Santor, n.d.; Elmer-DeWitt, 1990). The world's reliance upon computers was particularly demonstrated in the later years of the twentieth century when it was discovered that many older, critical software programs could not properly calculate dates after December 31, 1999. The concern over the Millennium Bug led directly to the expenditure of billions of dollars to update computer software to eliminate this problem (Dearlove, 2001). The viability of a business often depends upon the continual and reliable operation of its computer system. In addition, significant financial commitments are frequently made on the basis of computer-generated data.

The consequences of low-quality computer hardware and software are not infrequent or insubstantial. A recent report from the U.S. Department of Commerce states that total U.S. software sales in 2000 were approximately \$180 billion (RTI, 2002). The report estimated that the lack of an adequate software testing infrastructure costs U.S. software users over \$38 billion per year, principally through error avoidance and mitigation activities. The report also noted that these estimated costs do not reflect costs "...associated with mission critical software where the failure can lead to extremely high costs such as loss of life or catastrophic failure" (p. ES-3). The report further noted that roughly 22% of PCs break down every year—compared to 9% of VCRs; 7% of big-screen TVs; 7% of clothes dryers; and 8% of refrigerators.

In just about every instance, a computer system is acquired, software is used, or data are accessed through a contract-based commercial transaction. Therefore, whether a computer, software or data vendor will be held liable depends on the language of the contract itself and the law of contracts. As this chapter will discuss, most contracts impose scant liability for vendors. Aggrieved users have pursued other avenues of relief through noncontract-based legal theories, but with little success. For computer, software and data users, the Latin maxim of *caveat emptor* still applies—let the buyer beware.

BACKGROUND

Two of the principal sources of law in the American legal system are court decisions resulting from lawsuits and laws enacted by legislatures. A lawsuit is initiated by an aggrieved party—the plaintiff—filing a complaint with the appropriate court, which must be defended by the party or parties named in the complaint—the defendant (or defendants). Unless the case is settled by the parties, a trial is held at which evidence is presented and witnesses testify. Either party may appeal the decision of the trial to a higher court of appeals. The appeals court reviews the trial proceedings to determine whether the appropriate laws were applied correctly. No evidence or testimony is presented at the appeal.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/liability-system-data-quality/29313

Related Content

A Game Theoretical Approach to Design: A MAC Protocol for Wireless Sensor Networks

S. Mehta, B. H. Kim and K.S. Kwak (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 1475-1497).
www.irma-international.org/chapter/game-theoretical-approach-design/75087

Security of ICTs Supporting Healthcare Activities

José Manuel Gaivéo (2015). *Standards and Standardization: Concepts, Methodologies, Tools, and Applications* (pp. 192-212).
www.irma-international.org/chapter/security-of-icts-supporting-healthcare-activities/125293

Transport Layer for Cognitive Radio Sensor Networks

Yasir Saleem and Farrukh Salim (2015). *Standards and Standardization: Concepts, Methodologies, Tools, and Applications* (pp. 361-386).
www.irma-international.org/chapter/transport-layer-for-cognitive-radio-sensor-networks/125301

Standardising the Internet of Things: What the Experts Think

Kai Jakobs, Thomas Wagner and Kai Reimers (2011). *International Journal of IT Standards and Standardization Research* (pp. 63-67).
www.irma-international.org/article/standardising-internet-things/50575

Intellectual Property Protection and Process Modeling in Small Knowledge Intensive Enterprises

Riikka Kulmala and Juha Kettunen (2010). *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues* (pp. 151-167).
www.irma-international.org/chapter/intellectual-property-protection-process-modeling/43493