

Abstract

In 2008 alone, the Federal Trade Commission (FTC) settled five administrative complaints involving information security breach cases, under its unfair and deceptive practices jurisdiction. In these cases, tens of millions of consumer records were lost to unauthorized third parties. The FTC addressed security failures from diverse businesses and under unique factual circumstances; this paper examines the discrete set of fifteen security cases settled by the FTC between 2002 and 2008, to examine the relationship between security law, information security management, and consumer privacy. It describes the circumstances of the security lapses in chronological order, identifying the source of the security failure and the cause of the loss of information. As a result of this review, it can be seen that over time the FTC established consistent security measures, processes the authors' term Core Security Principles. The study of cases provides information longitudinally about the progression of security management. Additionally, the cases provide insight into the relationship between consumer privacy, law, and information security management. For consumer privacy to be realized, the authors recommend that the FTC expand its efforts to require businesses to implement secure information practices and that the private sector commit to due diligence in their security practices. Without regulatory and business cooperation to promote secure information use, consumer privacy will undoubtedly continue to be compromised in ways that are beyond individual control.