Abstract. Laws and regulations are playing an increasingly important role in requirements engineering and systems development. Monitoring systems for requirements and policy compliance has been recognized in the requirements engineering community as a key area for research. Similarly, legal compliance is critical in systems development, especially given that non-compliance can result in both financial and criminal penalties. Working with legal texts can be very challenging, however, because they contain numerous ambiguities, cross-references, domain-specific definitions, and acronyms, and are frequently amended via new statutes, regulations, and case law. Requirements engineers and compliance auditors must be able to identify relevant legal texts, extract requirements and other key concepts, and monitor compliance. This chapter surveys research efforts over the past 50 years in handling legal texts for systems development. This survey can aid requirements engineers and auditors to better specify, test, and monitor systems for compliance.

Keywords: legal requirements, legal compliance.

1 Introduction

Requirements for software systems are increasingly originating in laws and regulations. For example, numerous laws and regulations have emerged in the past fifteen years regarding data privacy. In the United States, privacy requirements have been elaborated by laws and regulations governing particular industries, such as the Health Insurance Portability and Accountability Act (HIPAA), which governs patient health records, and the Gramm-Leach-Bliley Act, which governs financial institutions. In Europe, the European Union passed the EU Directive on Data Protection, which details privacy requirements for all organizations operating in Europe. Several other countries, such as Canada with its passage of the Personal Information Protection and Electronic Documents Act, have enacted comprehensive privacy requirements cutting across all private-sector industries.

The need for system developers to monitor systems for both requirements and policy compliance has been identified as a challenging and important problem.
in the requirements engineering community [43]. According to recent surveys of senior information security professionals, legal compliance has been the primary driver of information security policy for the past three years [18]. Requirements engineers and system developers currently face two major problems in assessing legal compliance: (1) determining the applicable regulations, and (2) creating the requirements and policies necessary to achieve compliance with those regulations [25]. Methodologies for monitoring compliance with requirements and policies currently are not available to developers [43]. And yet, stakeholders need to better understand the regulations that govern the systems for which they are responsible and require precise answers to specific queries about what is allowed and what is not allowed [4][37]. The penalties for non-compliance can be severe; for example, HIPAA specifies up to $250,000 and 10 years in prison for criminal violations.

For requirements engineers, access to specific laws and regulations has become easier with the push towards online access for legal texts occurring in some countries. However, an organization must still identify the regulations relevant to its specific system before it can even begin to assess its compliance with the law. Once the relevant laws and regulations are identified, extracting requirements from legal texts is still a difficult and error-prone process [48]. In addition, an organization must still engage in traditional software engineering activities (e.g., analysis, modeling, development) as well as traditional security activities (e.g., policy enforcement and auditing) in order to properly implement legal compliance processes [15].

This chapter surveys research efforts over the past 50 years in modeling and using legal texts for system development. The survey identifies the strengths and weaknesses of each approach, and based on analysis of the literature to date as well as our prior experiences in analyzing policy and regulations [14][20][39], we propose a broad set of requirements for tool support that would aid requirements engineers and compliance auditors alike. It is our hope that these requirements will prompt serious consideration by the requirements engineering community, as it is within this community that we believe significant progress can be made to address the challenges related to legal compliance in software systems. The treatment of legal texts requires consideration of the business, organizational, and community context surrounding the development process in order for requirements engineers to appropriately address legal requirements.

The remainder of this chapter is organized as follows. Section 2 discusses the nature of legal texts, noting the various characteristics that make such texts difficult to work with. Section 3 discusses the three key layers of law relevant to requirements engineers in working with legal texts. Section 4 analyzes various efforts from the past 50 years in modeling regulations, extracting key concepts, and using legal texts in system development. Based on our extensive review of prior work, Section 5 proposes a set of broad requirements for comprehensive systems to assist requirements engineers and auditors with regulatory compliance tasks. Finally, Section 6 discusses the analysis and outlines future work needed to realize such systems.