

# Legal Requirements, Compliance and Practice: An Industry Case Study in Accessibility

Travis D. Breaux, Annie I. Antón  
Department of Computer Science  
North Carolina State University  
{tdbreaux,aianton}@ncsu.edu

Kent Boucher, Merlin Dorfman  
Cisco Systems, Inc.  
San Jose, California, USA  
{kboucher,mdorfman}@cisco.com

## Abstract

*U.S. laws and regulations are designed to support broad societal goals, such as accessibility, privacy and safety. To demonstrate that a product complies with these goals, businesses need to identify and refine legal requirements into product requirements and integrate the product requirements into their ongoing product design and testing processes. We report on an industry case study in which product requirements were specified to comply with Section 508 of the U.S. Workforce Investment Act (WIA) of 1998. This study sought to identify: limitations in existing requirements-acquisition methods; compliance gaps between previously specified product requirements and Section 508 of the WIA; and additional sources of knowledge that are necessary to refine legal requirements into product requirements to comply with the law. Our study reveals the need for a community of practice and generalizable techniques that can reduce ambiguity, complexity and redundancy in legal and product requirements and manage innovation in product requirements. We present these findings with several examples from Section 508 regulations and actual product requirements that are implemented in Cisco products.*

## 1. Introduction

In the United States, federal laws set minimum standards on business practices to achieve broad societal goals. Laws such as Section 255 of the 1996 Telecommunications Act<sup>1</sup> and Section 508 of the 1998 Workforce Investment Act<sup>2</sup> require federal agencies to provide access to electronic information to individuals with disabilities. Businesses that sell information access-related products, such as computer and software systems, to U.S. federal agencies must ensure their products satisfy the legal requirements of Sections 255 and 508. Because the public purchases the same products from companies such as Cisco, IBM, Oracle and Microsoft, the societal benefit of these laws is extended

to the general population. In the U.S., this includes 36.4 million adults who experience some hearing difficulty without a hearing aid, 20.2 million adults who report trouble seeing even with glasses or contact lenses, and 32.4 million adults who have limited reach or mobility [21]. Methods that improve a company's ability to comply with accessibility regulations will have a direct and positive effect on these individuals.

This paper reports the findings of an industry case study that analyzed product requirements developed to comply with Section 508 regulations, called the Accessibility Standards. The study includes a comparative evaluation between legal requirements acquired from the Accessibility Standards by North Carolina State University (NCSU) using the frame-based method [3] and product requirements that were originally developed by IBM and later refined, extended and contextualized for Cisco products by the Cisco Accessibility Team. The Cisco process used a *community of practice* — “a collective process of learning that coalesces in a shared enterprise” — such as improving accessibility for individuals with disabilities [25]. This evaluation identified method limitations, compliance gaps and additional sources of knowledge that affect how product developers comply with the law.

The remainder of the paper is organized as follows: Section 2 presents related work; Section 3 presents background on Section 508; Section 4 describes the NCSU and Cisco requirements, including how they were created; Section 5 presents the case study design; Section 6 presents summary findings; we conclude with key recommendations to practitioners in Section 7 and discussion and future work in Section 8.

## 2. Related Work

Recent efforts seek to model and catalogue legal requirements in privacy and corporate governance. Model-based approaches have been used to represent regulations as permissions and obligations [4, 20], check consistency of obligations and delegations [20], manage traceability between goal-based artifacts [11] and illustrate how businesses integrate compliance activities into their “daily work” [19]. In addition,

<sup>1</sup> Public Law No. 104-104, 110 Stat. 56 (1996)

<sup>2</sup> Public Law No. 105-220, 112 Stat. 936 (1998)

techniques have been proposed to help businesses organize legal requirements into a reusable catalogue [23] and prioritize legal requirements using stakeholder classes and a priority hierarchy for managing exceptions between requirements [3].

Breaux et al. propose a method to systematically acquire legal requirements from privacy regulations using formal models [3, 4]. The method provides heuristics for precisely mapping from regulatory phrases to legal requirements, called permissions, obligations and refrainments [3]. Herein, we apply it to a new domain, accessibility, and compare the resulting legal requirements with product requirements developed by Cisco.

Related efforts that focus specifically on legal requirements and accessibility law include the perspectives of technical writers [16], educators [17] and researchers investigating web-based compliance [18] and ubiquitous systems [12]. Jackson describes how Sun Microsystems developed its accessibility guidelines by coordinating product teams [16]. Section 5 describes how Cisco expands this work reaching out to a “community of practice” that includes potential users, accessibility experts, regulators and reporters.

Legal requirements directly impact product innovation and can potentially restrict or stifle innovation [24]. An alternative approach proposes learning from legal requirements in telecommunications accessibility to develop a ubiquitous computing innovation model [12]. Section 7 shows how developers can innovate within a legal framework by generalizing from legal requirements to legal goals to exceed compliance expectations.

### 3. Accessibility and Section 508

In the U.S., accessibility to electronic information by individuals with disabilities has evolved over the past two decades to keep pace with evolving technology. The primary impetus was Section 508 of the 1986 U.S. Rehabilitation Act Amendments<sup>3</sup>, which originally required manufacturers to develop guidelines “to insure that handicapped individuals may use electronic office equipment with or without special peripherals.” While this legal phrasing was in step with an office machination tradition, it lacked sufficient detail to address the many nuances of complex information systems that U.S. citizens would be using in the coming decade. Twelve years later, the 1998 Workforce Investment Act<sup>4</sup> increased the reach of Section 508 by extending access to “electronic and information technology” in general and requiring reporting, complaint and enforcement mechanisms to improve accountability. The statutes in both laws were limited to informa-

tion that was accessible through federal agencies and intentionally did not cover information shared by businesses that were not under federal contracts affecting individuals with disabilities.

In December 2000, the U.S. Architectural and Transportation Barriers Compliance Board (the Access Board) published the final regulatory rule, titled “Electronic and Information Technology Accessibility Standards” (the Accessibility Standards), for compliance with Section 508 [1]. These standards require technology companies seeking government procurement contracts to align the standards with their information technology products. The Accessibility Standards contain four subparts. Subpart A, titled “General,” includes the purpose, jurisdiction, exceptions and relevant legal definitions. Subpart B, “Technical Standards,” contains the following sections that include rules governing product classes:

§1194.21: Software applications and operating systems

§1194.22: Web-based intranet and Internet information and applications

§1194.23: Telecommunications products

§1194.24: Video and multimedia products

§1194.25: Self-contained, closed products

§1194.26: Desktop and portable computers

Subpart C, “Functional Performance Criteria,” includes broad requirements that focus developers’ attention on specific disabilities, including difficulty in hearing, speaking and seeing and a lack of fine motor control or simultaneous action. Subpart D, “Information, Documentation and Support,” requires that documentation and product support be provided via alternative methods and formats that individuals with disabilities can access.

### 4. Accessibility Requirements

To comply with the Accessibility Standards, developers must align their products with legal requirements. This case study compares legal requirements acquired by NCSU using a frame-based method and product requirements developed by IBM and Cisco as we now discuss.

#### 4.1. NCSU Accessibility Requirements

The NCSU accessibility requirements were acquired using the frame-based requirements analysis method (FBRAM), which builds on existing goal-based analysis methods by partitioning natural language phrases from requirements statements into categories, called *case roles*, that have a consistent meaning [3]. This partitioning, called *semantic parameterization*, provides businesses with a strict focus and standard procedure by which they can interpret regula-

<sup>3</sup> Public Law No. 105-220, 112 Stat. 936 (1998)

<sup>4</sup> Public Law No. 99-506, 110 Stat. 1807 (1986)

tions while preserving traceability. This additional emphasis moves businesses toward a position that is legally defensible and sustainable with changing societal and technological norms. The FBRAM has been applied to the HIPAA Privacy Rule to identify privacy and security requirements using a tabular format [3]. To illustrate the method, consider the following excerpt from Section 508:

**Subpart B, §1194.21(d):** When an image represents a program element, the information conveyed by the image **must** also *be available* in text.

Figure 1 represents this excerpt as a frame-based requirement. The excerpt phrases are classified into case roles, called *properties*. The modal phrase “must” indicates this statement is an obligation. The action phrase “be available” is restated from passive to active voice as “make available.”

| Record Number: 27 |            |   |
|-------------------|------------|---|
| Paragraph         | Property   | Value   |
| 1194.21(d)        | Pre-con    | When... an image represents a program element |
| 1194.21(d)        | Object     | Information conveyed by the image             |
| 1194.21(d)        | Modality   | Obligation                                    |
| 1194.21(d)        | Action     | Make available                                |
| 1194.21(d)        | Instrument | In... text                                    |

**Figure 1: Requirements frame example**

In addition to parameterizing and itemizing legal requirements, exceptions to requirements are documented in a separate priorities table that helps engineers determine which requirements apply to a specific context [3]. Requirements captured in the tabular format are presented using a standard sentence schema, a process called *normalization*, which represents relevant roles for a given action. In this paper, we present the NCSU requirements as normalized statements with the action word(s) capitalized. For example, the requirement in Figure 1 is normalized using the schema: [ACTION] [object] [instrument] [purpose], [condition] as follows:

**NCSU O-27:** MAKE AVAILABLE information conveyed by the image in text, when an image represents a program element.

In this paper, the modality role is encoded in the requirement identifier; for example, the “O” in O-27 stands for “obligation,” “P” stands for “permission,” and “R” stands for “refrainment.”

#### 4.2. Cisco Accessibility Requirements

The Cisco Accessibility Team developed the Cisco accessibility requirements, in conjunction with Inclusive Technologies, a company that provides domain

expertise, market research and training on accessibility-related issues [22]. This approach connected Cisco with a *community of practice*, which is “a collective process of learning that coalesces in a shared enterprise,” such as improving accessibility for individuals with disabilities [25]. Communities of practice emerge to address social problems that extend beyond the experiences or sphere of influence of any one individual. In a process of collective learning, these communities negotiate or refine meaning through participation and reification (the grounding of abstract concepts in the form of concrete experiences). The duality of participation and reification enables the community to extend and refine knowledge of the shared enterprise to be inclusive of diverse opinion and to create explicit knowledge from tacit experience. Because accessibility issues affect individuals differently and evolve in step with new technology, engagement with a community of practice is critical for meeting or exceeding regulatory expectations.

Cisco initially considered three basic approaches to comply with the Accessibility Standards : (1) use the original framework contained in the Sections 255 and 508; (2) customize accessibility requirements published online by IBM [14]; or (3) develop a unique structure [22]. Whereas the decision was made to customize the IBM requirements, Cisco first identified relevant Cisco products and contextualized the regulations based on relevant product features. For example, the Accessibility Standards require using “alt” tags for displaying bitmap images on web pages. Whereas IBM develops products that allow users to author and display web pages, Cisco products did not provide web page authoring features at the time, and thus IBM requirements that focused on these capabilities could be ignored by Cisco [22].

In addition to contextualization, Cisco monitored changes of regulatory interpretations in public forums. These changes often coincide with the development of new technologies. For example, the Accessibility Standards require the ability to disable scripts in web pages because electronic screen readers, which parse and speak textual information for the visually impaired, initially experienced difficulty parsing these scripts from within HTML. However, screen readers today have overcome this challenge, thus scripts are not typically disabled<sup>5</sup>. Similar improvements in other technologies can change how industry prioritizes compliance with regulations.

Cisco also used the community of practice to identify areas of the regulation where public sensitivity was

<sup>5</sup> However, AJAX and Web 2.0 have recreated a similar technological challenge for screen readers; thus the relevance of this requirement is returning.

high by monitoring and collating information from the U.S. General Services Administration (GSA), which has an enforcement arm, and from the Access Board, newspapers, public sector IT publications such as *Federal Computer Week*, trade shows, web logs, etc.

One noteworthy challenge for all stakeholders seeking to comply with U.S. law is that regulatory guidance is often provided by government agencies in proportion to interest from the current presidential administration. The focus on compliance, including how statutory law is implemented and enforced, may differ in executive branch departments and agencies. In recent years, lax enforcement in the U.S. has shifted manufacturers' focus toward the European Community, which is developing accessibility regulations to govern multiple sectors, including education, telecommunications, and transportation [22]. U.S. businesses should be wary, however, because during periods of lax enforcement, the oversight of compliance shifts toward checklists and other summary tactics that substitute for comprehensive and detailed requirements specification and testing. In future years, should enforcement re-emerge as a presidential priority, significant product re-engineering may be required to ensure that products comply with more rigorous enforcement procedures.

## 5. Comparative Case Study Design

To investigate differences that exist between legal and product requirements in one domain, we employed an exploratory, single case study design [26] intended to yield constructivist knowledge claims and to discover outcomes (as opposed to examining underlying causes) [7]. Unlike controlled experiments designed to accept or reject specific hypotheses that have a narrow focus, this design is necessary to answer research questions that have a broad focus and to discover new theory. This section presents our research questions, discusses the units of analysis and materials used to answer these questions, and introduces the metrics used to identify propositions that link the data to the findings in Sections 6 and 7.

### 5.1. Research Questions

The objective of this case study is to understand and evaluate one company's attempt to align its product development with legal requirements and to generalize this understanding into insightful best practices. We focused this investigation on answering three research questions (RQs):

**RQ<sub>1</sub>:** What kinds of gaps exist, if any, between the Cisco and NCSU requirements and the Accessibility Standards?

**RQ<sub>2</sub>:** How are product requirements written to exceed the Accessibility Standards, or how do they fall short of compliance?

**RQ<sub>3</sub>:** What knowledge sources are needed to reduce legal ambiguity when refining legal requirements for product development?

To answer research question RQ<sub>1</sub>, we defined "gap" as follows: a "gap" exists if: (1) there is a requirement in one requirements set (NCSU or Cisco) that does not appear in the other set; or (2) there is a paragraph in the Accessibility Standards that is not cross-referenced to an NCSU or Cisco requirement.

To identify the first type of gap, we must empirically compare two requirements. A coarse-grained comparison can be achieved by simply classifying pairs of requirements into one of two categories: similar or dissimilar. However, this approach has several limitations. First, it does not require the investigator to think critically about the significance of subtle semantic differences or similarities and, therefore, it does not sufficiently discriminate to identify the different "kinds" of gaps that may potentially exist between two requirements sets. For example, consider two phrases: "controls and keys" and "physical controls." These are similar, because both phrases describe "controls," but they are also dissimilar, because one phrase describes "physical" controls and excludes the term "keys." Differences like these can further determine whether a requirement is written to exceed compliance or if it falls short, thus providing important insight to help answer research question RQ<sub>2</sub>. Second, this approach does not capture the investigators' rationale for categorizing two requirements as similar or dissimilar. To improve the reliability of our findings, we are interested in surfacing, rationalizing, representing and preserving the investigator's structured argument about why two requirements are comparable in the form of logical assertions for later independent review. To address this semantic subtlety and improve experimental rigor, we developed metrics that require the investigators to think critically when they compare requirements by presenting justification in the form of logical assertions.

Finally, to identify the second type of gap, we overlay the traceability data (cross-references between regulatory paragraphs and unique requirements) from Cisco with the NCSU traceability data maintained by the FBRAM. Because the FBRAM rigorously acquires requirements directly from the paragraph text while maintaining indices to this original text, the FBRAM traceability data is highly reliable.

### 5.2. Units of Analysis and Materials

The units of analysis in our design for this study consist of natural-language requirement statements and phrases and traceability data that associate these requirements to paragraphs in the regulation.

The case study materials consist of two sets of requirements, one provided by NCSU and the other provided by Cisco. The NCSU requirements were acquired from the Accessibility Standards, Subparts A-D, using the FBRAM tabular format [3]. The first author performed this procedure across five sessions that spanned 10.5 hours to yield 141 requirements. The NCSU requirements are organized according to the subpart title and product category, if any, that appear in the Accessibility Standards. The Cisco accessibility requirements refine and extend a subset of 105 accessibility requirements previously published online by IBM [14]. This process consumed over 120 hours spent by four people. The Cisco requirements are organized into the following categories: Browser-based, Business Practices, Documentation, Hardware, Non-browser-based and Telephony.

Each Cisco requirement is formatted using a standard template. The template includes a unique index, a single natural-language requirement definition, a requirement level or modality (e.g., “must,” “should”), a rationale, including user scenarios, and a requirement specification that consists of one or more numbered mandatory and optional techniques and examples that demonstrate how the requirement should or can be implemented. Our study was limited to the requirement definition (called “first tier” requirements) and the numbered techniques (called “second tier” requirements); in total, this limited focus yielded 389 requirement statements. Cisco also provided a concordance that maps each first-tier requirement to a paragraph in Subparts B, C and D of the Accessibility Standards. Currently, the Cisco requirements documents and concordance consists of 180 pages and more than 35,000 words of technical material; the restricted focus used only 47% of this material.

Finally, we interviewed Jim Tobias, the lead coordinator and CEO of Inclusive Technologies. This interview provided important background to the Cisco product requirements development process and the regulatory environment discussed in Section 4.2.

### 5.3. Metrics for Comparing Requirements

Because informal comparisons can be subjective and affected by individual bias, we developed and employed a set of qualitative metrics that investigators use to rationalize the comparison of two requirements. The metrics are intended to direct the investigator’s focus to evaluate subtle differences in meaning. Unlike software quality metrics that yield numerical measurements [15], our metrics yield nominal measurements in the form of logical assertions. We analyze these measurements to identify propositions that link the data to our findings through pattern-based inferences [5]. These patterns consist of constant features (the type of

assertion) and the manner by which assertions of the same type coordinate variable features in the observable phenomena (the requirements statements and their phrases). We now discuss the metrics in the context of comparing two arbitrary requirements, A and B.

**5.3.1. Statement Metrics.** The statement metrics are used to compare two requirement statements, avoiding a detailed evaluation of differences between specific phrases or words in those statements. The metrics are:

**Metric S-G (Goal):** Requirement A describes “why” Requirement B should be implemented.

**Metric S-R (Refinement):** Requirement A describes “how” Requirement B should be implemented.

**Metric S-E (Equivalent):** Requirements A and B are equivalent, with some portions of the requirements describing the same or a similar action.

Metrics S-G and S-R are based upon the concept of goal refinement in goal-oriented requirements acquisition [8]. Table 1 presents an example from our case study that shows the above statement metrics applied to obligation NCSU O-29 (Requirement A) and three Cisco requirements (Requirements B). We include the original text from §1194.21(f) in the Accessibility Standards from which NCSU O-29 was acquired:

**§1194.21(f):** Textual information shall be provided through operating system functions for displaying text.

**NCSU O-29:** PROVIDE textual information through operating system functions for displaying text.

**Cisco SW-50.11:** Provide text in a manner compatible with assistive technology.

**Cisco SW-50.11 (M2):** Draw text using the standard function calls; this applies to text in the client area as well as text in custom controls

**Cisco SW-50.11 (M3):** Use standard functions to copy or erase text and graphics.

**Table 1: Statement-level metrics applied to NCSU-Cisco requirements pairs**

| NCSU Req’t | Cisco Req’t   | Metric |
|------------|---------------|--------|
| O-29       | SW-50.11      | S-G    |
| O-29       | SW-50.11 (M2) | S-E    |
| O-29       | SW-50.11 (M3) | S-R    |

**5.3.2. Phrase Metrics.** The phrase metrics are used to compare discrete phrases in two requirements. These metrics are used in conjunction with one of the above statement metrics to further clarify the similarity or difference in a requirements’ meaning. They are:

**Metric P-G1 (Generalized Concept):** The “phrase in B” describes a more general concept than the “phrase in A.”

**Metric P-G2 (Missing Constraint):** The “phrase in A” is missing from Requirement B.

**Metric P-R1 (Refined Concept):** The “phrase in B” describes a more refined concept than the “phrase in A.”

**Metric P-R2 (New Constraint):** The “phrase in B” is missing from Requirement A.

**Metric P-M (Modality Change):** The “phrase in A” has a different modality than the “phrase in B.”

For each applicable phrase metric, the investigator creates a corresponding assertion that includes the original phrases from both requirements that justify the metric’s application. The assertions are documented and preserved for traceability and later reviewed by other investigators. For example, the obligation NCSU O-29 (Requirement A) is compared with Cisco requirement SW-50.11 (M2) (Requirement B) to yield the following phrase metric assertions  $A_1$ - $A_4$ :

**A<sub>1</sub> (P-G1):** Generalizes from “through operating system functions for displaying text” to “using the standard function calls”

**A<sub>2</sub> (P-R1):** Refines from “textual information” to “text”

**A<sub>3</sub> (P-R1):** Refines from “be provided” to “draw”

**A<sub>4</sub> (P-R2):** Refines to include “this applies to text in the client area as well as text in custom controls”

The statement metrics S-R and S-G and phrase metrics P-R and P-G are symmetric. To illustrate, consider the assertion  $A_5$  (below), which is symmetric with  $A_2$  (above) and which would result from inversely comparing Cisco SW-50.11 (M2) to NCSU O-29:

**A<sub>5</sub> (P-G1):** Generalizes from “text” to “textual information”

The eight metrics were refined in a pilot study using 105 accessibility requirements developed by IBM. We empirically validated the three statement metrics using two inter-rater reliability statistics for nominal data: Cohen’s Kappa for two raters [6] and Fleiss’ Kappa for multiple raters [9]. The Cohen and Fleiss Kappa statistics are a value [0,1] and measure the actual observed agreement among raters (P) excluding the expected agreement ( $P_e$ ), if agreement were due strictly to chance, and is expressed by the formula:  $\kappa = (P - P_e) / (1 - P_e)$  [6, 9]. For Fleiss’ Kappa, we used a stratified sample of legal and product requirements and four raters who are all graduate students enrolled in a requirements engineering course. We observed a 61.2% probability that the agreement among four raters occurred beyond what is expected by chance. For Cohen’s Kappa and the same stratified sample, we observed that the first author and three of the four raters were in agreement 70-80% beyond what is expected by chance.

Different factors, including the survey instrument, number of categories and number of raters, influence the Kappa statistics. We could not evaluate the phrase metrics using the Kappa statistics, however, because these metrics are not exclusive (i.e., a requirement pair may be classified by multiple phrase metrics).

#### 5.4. Analysis and Interpretation Procedure

In this study, we performed a *gap analysis*, which is used in corporate governance to compare current performance with expected or desirable performance [13]. The gap analysis entails applying the metrics to the Cisco and NCSU requirements and then inferring alignments between Cisco requirements and the Accessibility Standards from assertions identified by the metrics. These inferred alignments are overlaid with the Cisco concordance to identify gaps, if any.

The metrics were applied by performing a pair-wise comparison between Cisco and NCSU requirements sets. In practice, the investigator begins by trying to apply metric S-E to two requirements, one from each set. If this fails, he or she subsequently tries to apply metrics S-R and S-G before concluding the statements are not comparable; this result may be due to the investigator’s having insufficient domain knowledge.

## 6. Summary Findings

The application of the metrics described in Section 5.3 to the NCSU and Cisco requirements resulted in a total 635 mappings: 354 refinements (S-R), 31 generalizations (S-G), and 250 similar actions (S-E). Thirty-eight NCSU requirements and 19 Cisco requirements did not map between the sets. However, every paragraph in the Accessibility Standards aligned with at least one NCSU and one Cisco requirement. The study also yielded 555 phrase assertions, including 183 refined concepts (P-R1), 50 new constraints (P-R2), 134 generalized concepts (P-G1), 132 missing constraints (P-G2) and 56 modality changes (P-M) among the Cisco requirements. None of the Cisco requirements were “true refinements,” (that is, if the S-R metric applies, then only P-R metrics apply) or “true generalizations” (that is, if the S-G metric applies, then only P-G metrics apply). This finding is especially interesting because it demonstrates the challenge that developers and regulators face: contextualizing product requirements provides needed guidance to engineers, yet, this introduces new wordings that simultaneously refine and generalize regulatory concepts and terms.

Table 2 presents an example from the gap analysis. The columns map to Cisco requirements in which the first-tier requirement SW-50.11 appears in the first R column, followed by its associated second-tier requirements, M1, M2, M3 and so on. The rows map to paragraphs in the Accessibility Standards. Cells are

marked as follows: (C) Cisco identified an alignment between the Cisco requirements and the Accessibility Standards; (N) NCSU identified an alignment between the Cisco requirements and the NCSU requirements, thus inferring an alignment with the Accessibility Standards; or (B) both Cisco and NCSU alignments were identified for this requirement.

**Table 2: Example of regulatory gap analysis for Cisco software requirements**

| Section 508 | SW-50.11 |    |    |    |    | SW-50.21 |   |    |    |
|-------------|----------|----|----|----|----|----------|---|----|----|
|             | R        | M1 | M2 | M3 | M4 | M5       | R | M1 | M2 |
| 1194.21(b)  | C        |    |    |    |    |          |   |    |    |
| 1194.21(d)  |          |    |    |    | N  |          |   | N  |    |
| 1194.21(f)  | B        | N  | N  | N  | N  |          |   |    |    |
| 1194.21(i)  |          |    |    |    |    |          | B |    |    |
| 1194.21(c)  |          |    |    |    |    |          | N |    |    |
| 1194.31(a)  | N        | N  | N  | N  | N  |          | C |    |    |
| 1194.31(b)  | N        | N  | N  | N  | N  |          | C |    |    |
| 1194.31(c)  |          |    |    |    |    |          | C |    |    |

The gap analysis yielded interesting results. First, the Cisco concordance data uses a coarse-grained classification, in which only first-tier requirements were mapped to paragraph references in the Accessibility Standards. For this reason, this study revealed 198% additional conformance between the Accessibility Standards and the Cisco requirements that did not appear in the Cisco concordance. This coverage is exemplified in Table 2 as shaded mappings from SW-50.11 (M1-M4) crossed with §1194.21(d)-(f). In addition, we found an inconsistent alignment between NCSU and Cisco requirements and the functional performance criteria in §1194.31(a)-(c), also shaded in Table 2. This inconsistency is avoidable because these paragraphs internally align with other paragraphs in the Accessibility Standards, as demonstrated by applying our metrics S-R and S-G in a separate analysis motivated by this result. Thus, if we align a requirement with paragraph §1194.21(f), which requires providing textual information via accessible technology, we can immediately infer that this requirement also aligns with paragraph §1194.31(a), which requires at least one mode of operation for users with limited visual acuity. These inferences constitute undocumented redundancies within the Accessibility Standards themselves.

In contrast to the HIPAA, which was written and organized with stakeholders as the primary focus [3, 4], the Accessibility Standards are organized according to a *product focus*. The product vs. stakeholder focus prominently affects how engineers write their product requirements. For example, we observed that only 34% of the NCSU requirements explicitly state the subject because of ambiguities present in the Accessibility Standards. This under-specification requires developers to determine whether the subject of these requirements is a product and its functions or a stakeholder and their

actions. For example, §1194.21(c) requires a focus that “that moves among interactive interface elements as the input focus changes” but does not indicate what subject is changing the focus, the product or the user.

Another observation that coincides with the product focus is that the standards are organized around classes of products as opposed to product features. For example, the Accessibility Standards include three classes for products that qualify as software applications (§1194.21), web applications (§1193.22) and telecommunications products (§1194.23). For innovative products, such as voice-over-IP (VoIP) products that allow users to make voice calls over the Internet and that use a web-based interface, compliance with each class of rules is necessary. We identified 55 redundancies across product classes, classified by the S-E metric, in the Accessibility Standards.

## 7. Compliance Patterns

The gap analysis resulted in logical assertions that rationalize similarities and differences between legal and product requirements. Sorting these assertions by metric type enabled us to identify compliance patterns. A few of these patterns capitalize on our earlier observations that some legal requirements are refrainments [3]. We believe these patterns will help regulators to write clearer regulations and assist product developers to improve compliance coverage and manage innovation. The patterns are organized under two themes *simplification* and *clarification*, which we now present; at the end of each sub-section, we conclude with a recommendation in *italics*.

### 7.1. Simplifying Compliance

Legal requirements are written to achieve societal goals. Regulators write legal requirements with complex conditions to focus the impact and moderate the frequency with which these rules must be enforced. We observe two techniques that developers can apply to simplify compliance by reacting to these conditions.

#### 7.1.1. Remove or Generalize Preconditions

Preconditions in legal requirements are presented in different ways: they appear as phrases that follow condition keywords (“if,” “when,”) or as classes of things to which requirements apply. Removing these phrases or generalizing these classes when writing product requirements yield interpretations of legal requirements with broader applicability in practice. This technique may cause developers to implement the product requirement more often than necessary. However, it may better achieve the intent of the societal goal or better protect the developer and company when their products innovate in ways unforeseen by regulators.

This pattern appeared in requirements pairs that were classified by the S-E metric and either the P-G1

or P-G2 metrics. To illustrate, consider the pair obligation NCSU O-73 and Cisco requirement HW-10.11 (M1), which were identified using metric S-E:

**NCSU O-73:** OPERATE telecommunications products, which have mechanically operated controls or keys with one hand...

**Cisco HW-10.11 (M1):** All physical controls must be activated by one hand...

We identified the following assertions, A<sub>6</sub> and A<sub>7</sub>, using the phrase metrics. Assertion A<sub>6</sub> corresponds to removing the association between controls and telecommunication products, in particular. Without this precondition, Cisco HW-10.11 applies to any product with physical controls. On the other hand, the phrase “physical controls” in assertion A<sub>7</sub> is a more general class of controls than “mechanically operated controls” because it includes electronic controls that appear on touch-screen displays.

**A<sub>6</sub> (P-G2):** Generalizes to remove precondition “telecommunications products that have mechanically operated controls or keys”

**A<sub>7</sub> (P-G1):** Generalizes from “mechanically operated controls” to “physical controls”

*Developers can reduce potential violations by removing preconditions or generalizing terms in permissions and obligations, at the cost of exceeding legal requirements. However, for products not covered by the law, these added costs may be difficult to justify.*

### 7.1.2. Preclude Preconditions / Assume Exceptions

Another approach to simplifying compliance involves writing product requirements so that they preclude satisfying legal preconditions. Assuming that the exception is true in a legal requirement will yield a similar effect. This technique applies to preconditions in the form of phrases that follow condition keywords (“if,” “when”) and exception keywords (“unless,” “except”). This pattern appears in requirements identified with the statement metric S-E and phrase metric P-M. Consider the following obligation NCSU O-53 and requirement Cisco WEB-40.10 (O1):

**NCSU O-54:** *When a timed response is required,* GIVE the user sufficient time to indicate more time is required.

**Cisco WEB-40.10 (O1):** Use no timed response elements.

In NCSU O-54, the precondition to “require” a timed response implies the obligated act of “using” a timed response; this is the shared action with Cisco WEB-40.10 to which the S-E metric applies. The assertion A<sub>8</sub> codifies the change in modality.

**A<sub>8</sub> (P-M):** Changes modality from an obligation to a refrainment

Because Cisco WEB-40.10 assumes the legal precondition in NCSU O-54 is not satisfiable, the Cisco requirement precludes the need to account for additional product functionality: in this case, giving the user sufficient time to indicate more time is required.

*Developers can reduce compliance efforts by creating a product requirement that precludes satisfying legal preconditions or assumes satisfying legal exceptions. However, this may be impractical if no cost-effective alternatives exist.*

## 7.2. Clarifying Compliance

Legal requirements contain intended and unintended ambiguities [2]. Intended ambiguities include legal terms that are chosen because they have broad meanings that account for known variability in the marketplace. Other ambiguities, intended or not, result from missing domain knowledge, which provides important rationale for legal requirements or describes contrary situations (e.g., conflicts) to legal requirements. We now demonstrate how developers can clarify legal requirements by resolving ambiguities through their product requirements.

### 7.2.1. Ground Legal Terms in the Domain

In government laws and regulations, a *term of art* is a precise phrase that has a specialized meaning in a specific subject area [10]. The meaning of these terms in a domain is refined by variants (other terms) that are known to practitioners. With regard to computer technology, new variants are introduced as companies develop new products. For example, the term of art “telecommunications,” which appeared as a term of art in Section 508 in the late 1980s, was later refined by the variant “voice-over-IP” in the late 1990s. Consider the following obligation NCSU 22, which is paired with the requirement (not shown) Cisco SW-10.21 (M1), using the S-E metric.

**NCSU 22:** AVOID DISRUPTING activated features of any operating system that are identified as accessibility features...

The Cisco requirement SW-10.21 (M1) contains phrases that were used to identify four logical assertions A<sub>9</sub>-A<sub>13</sub> of the following form:

**A<sub>9</sub>-A<sub>13</sub> (P-R1):** Refines “accessibility features of any operating system” to be each of:

- StickyKeys - to activate simultaneous keys
- FilterKeys - to control key repeat rate
- ToggleKeys - to hear tones when pressing key locks
- MouseKeys - to move mouse pointer via arrow keys

The terms StickyKeys, FilterKeys, ToggleKeys and MouseKeys are variants of the legal term “accessibility features” and are used across multiple operating systems, including Microsoft Windows XP and Mac OS X

version 10.4 (Tiger). The metric P-R1 frequently coincides with identifying these variants in statements coded with any of the S-G, S-R and S-E metrics.

*Developers should identify important terms of art and maintain and update lists of variants that must be addressed by their product requirements over time.*

### 7.2.2. Refine by Refrainment

Legal requirements may emphasize what products or stakeholders are permitted or required to do, but may not (intentionally or otherwise) anticipate many ways in which these requirements can be violated. Among requirements coded with the S-R metric are refinements that change the modality from a permission or obligation to a refrainment, coded by the P-M metric. These refrainments may include requirements intended to address such violations by resolving conflicts. To illustrate, consider the requirements Cisco SW-50.11 (M3) and Cisco SW-50.11 (M4), which were individually paired with obligation NCSU O-29 using the S-R metric.

**NCSU O-29:** PROVIDE textual information through operating system functions for displaying text.

**Cisco SW-50.11 (M3):** Avoid directly manipulating bitmaps.

**Cisco SW-50.11 (M4):** Avoid directly modifying the screen.

The rationale for why the Cisco requirements avoid violating NCSU O-29 is that some applications directly manipulate the memory associated with a device context, such as bitmaps and other graphics displays. In these situations, screen readers are not aware of the changes taking place and, therefore, they cannot communicate to the visually impaired the result or meaning of such manipulations.

*By codifying conflicts with legal requirements as refrainments, developers increase their assurance of avoiding unintended violations of law.*

### 7.2.3 Reveal the Regulatory Goal

Laws and regulations often include brief discussions of broad societal goals, but these discussions are not sufficiently comprehensive to include specific sub-goals. For example, consider requirement Cisco WEB-10.30, which is paired with the three obligations NCSU O-41, O-51 and O-52 using metric S-G.

**NCSU O-41:** PROVIDE redundant text links for each active region of a server-side image map.

**NCSU O-51:** ALLOW people using assistive technology to access the information, field elements, and functionality required for completion and submission of the [electronic] form, including all directions and cues.

**NCSU O-52:** PROVIDE a method that permits users to skip repetitive navigation links.

**Cisco WEB-10.30:** Provide sufficient methods for screen reader users to navigate easily and [to] complete forms.

Each of these NCSU obligations refines different “methods” that screen readers can use to achieve the Cisco requirement; however, the Accessibility Standards never make this goal explicit. This unstated goal provides developers important context and rationale to understand that screen readers are a target technology for testing implementations.

*Developers can increase compliance assurance in product implementations by identifying and codifying the unstated goals of legal requirements and using them to group related product requirements.*

## 8. Discussion and Summary

The comparative evaluation of the NCSU and Cisco requirements generated important insights that answer, in part, our three original research questions.

Research question RQ<sub>1</sub> asks what different types of gaps between legal and product requirements exist. Section 7.2 discusses three recommendations under the clarification theme. Each recommendation introduces new domain knowledge that is missing from the regulations. For example, the legal goals broadly affect multiple industries and organize manufacturer’s product requirements, whereas the domain terms and refrainments contextualize legal requirements to address specific products. Identifying and filling these gaps provides a more complete and comprehensible compliance landscape to developers.

RQ<sub>2</sub> asks how product requirements exceed or fall short of compliance. Section 7.1 discusses two recommendations under the simplification theme. By removing preconditions, developers can “play it safe” and exceed compliance by broadening the applicable scope of legal requirements. In contrast, by precluding preconditions and assuming exceptions, developers can systematically avoid having to satisfy additional legal requirements. Both approaches have associated costs, such as over-restricted or excessive product features with the benefit of compliance simplification.

RQ<sub>3</sub> asks what sources of knowledge were required to refine legal requirements and reduce legal ambiguity. Section 7.2 discusses the clarification theme and corresponding recommendations, showing how to apply domain terms from the community of practice to reduce ambiguity by refinement. Similar communities exist in domains associated with other quality requirements, including aerospace and medical safety, privacy and security. The legal, social and economic consequences of non-compliance, the danger to innovation from over regulation and the subjective limits on standards of care all necessitate a community of practice to

rationalize the complexity of legal compliance in these domains.

Finally, the gap analysis revealed that paragraphs in regulations contain multiple legal requirements and that a method similar to the FBRAM, which itemizes requirements and preserves legal language, is useful to incorporate legal requirements into a manufacturer's compliance framework. Our metrics demonstrate that alignments between legal and product requirements can be described in greater detail by using the goal-oriented concept of refinement. This concept can be employed systematically by following our recommendations in Section 7. Combined with a community of practice, the FBRAM and related techniques can improve how companies demonstrate due diligence and good faith under the law.

This paper presents an industry case study that demonstrates how to identify compliance gaps through the use of metrics for comparing requirements. The study resulted in five key recommendations identified from real world, product requirements. While this study was qualitative and exploratory by design, it revealed practical issues that we plan to further investigate with controlled experimentation.

### Acknowledgements

We thank Jim Tobias for his contributions. This work was supported by the IBM PhD Fellowship (RTP CAS), NSF #032-5269 and NSF #043-0166.

### References

- [1] "Electronic and information technology accessibility standards," 36 CFR Part 1194, *U.S. Federal Register*, 65(246): 80500-80528, Dec. 2000.
- [2] T.D. Breaux, A.I. Antón. "A systematic method for acquiring regulatory requirements: a frame-based approach," *6<sup>th</sup> Int'l Workshop on Req'ts for High Assurance Systems*, Delhi, India, 2007.
- [3] T.D. Breaux, A.I. Antón. "Analyzing regulatory rules for privacy and security requirements," *IEEE Trans. Soft. Engr., Special Issue on Soft. Engr. for Secure Sys.*, 34(1): 5-20, 2008.
- [4] T.D. Breaux, M.W. Vail, A.I. Antón. "Towards compliance: extracting rights and obligations to align requirements with regulations," *IEEE Int'l Conf. Req'ts Engr.*, pp. 49-58, 2006.
- [5] D.T. Campbell, "Pattern matching as an essential in distal knowing," *The Psychology of Egon Brunswick*. Holt, Rinehart, Winston. pp. 81-106, 1966.
- [6] J. Cohen. "A coefficient of agreement for nominal scales," *Educational and Psychological Measurement*, 20: 37-46, 1960.
- [7] J.W. Creswell. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, 2<sup>nd</sup> ed., Sage Pubs., 2003.
- [8] A. Dardenne, A. van Lamsweerde and S. Fickas, "Goal-Directed Requirements Acquisition." *Science of Computer Programming*, 20: 3-50, 1993.
- [9] J.L. Fleiss, "Measuring nominal scale agreement among many raters," *Psychological Bulletin*, 76(5): 378-382, 1971
- [10] B.A. Garner, *Black's Law Dictionary*, 8<sup>th</sup> ed., Thompson West, 2004.
- [11] S. Ghanavati, D. Amyot, L. Peyton, "Towards a framework for tracking legal compliance in healthcare," *19<sup>th</sup> Int'l Conf. Adv. Info. Sys. Engr.*, pp. 218-232, 2007.
- [12] R.A. Guedj, "Law and regulation to include elderly in innovations stream," *EC/NSF Workshop on Universal Accessibility of Ubiquitous Comp.*, pp. 111-114, 2001.
- [13] M.I. Harrison, M. Shirom, *Organizational diagnosis and assessment: bridging theory and practice*, Sage Pubs., 1999.
- [14] IBM Human Ability and Accessibility Center, Developer Guidelines; Jan. 2008; <http://www.ibm.com/able/guidelines/>
- [15] IEEE Std. 1061-1998 – Standard for a Software Quality Metrics Methodology
- [16] S. Jackson, "How interdisciplinary teams created company-wide section 508 guidelines for writers," *21<sup>st</sup> Int'l Conf. on Documentation*, pp. 140-142, 2003.
- [17] S. Ludi, "Introducing accessibility requirements through external stakeholder utilization in an undergraduate requirements engineering course," *IEEE 29<sup>th</sup> Int'l Conf. Soft. Engr.* pp. 736-743, 2007.
- [18] S.K. Kane, J.A. Shulman, T.J. Shockley, R.E. Ladner. "A web accessibility report card for top international university web sites," *Int'l Cross-Disciplinary Conf. on Web Accessibility*, pp. 148-156, 2007.
- [19] D. Karagiannis, J. Mylopoulos, M. Schwab. "Business process-based regulatory compliance: the case of the Sarbanes-Oxley act," *IEEE Int'l Req'ts Engr. Conf.*, pp. 315-321, 2007.
- [20] F. Massacci, M. Prest and N. Zannone. "Using a security requirements engineering methodology in practice: the compliance with the Italian data protection legislation," *Computer Standards & Interfaces*, 27(5):445-455, 2005.
- [21] J.R. Pleis, M. Lethbridge-Çejku. "Summary health statistics for U.S. adults: national health interview survey, 2005" *Vital and Health Statistics*, 10(232): 2006.
- [22] J. Tobias, personal communication, Dec. 2007
- [23] S. Toval, A. Olmos, M. Piattini. "Legal requirements reuse: a critical success factor for requirements quality and personal data protection," *IEEE Int'l Conf. Req'ts Engr.*, pp. 95-103, 2002.
- [24] N.L. Tsilas. "Enabling open innovation and interoperability: recommendations for policy-makers," *ACM 1<sup>st</sup> Int'l Conf. on Theory and Practice in Electronic Governance*, pp. 53-56, 2007.
- [25] E. Wenger. *Communities of Practice: Learning, meaning, and identity*, Cambridge University Press, 1998.
- [26] R.K. Yin. *Case Study Research*, 3<sup>rd</sup> ed. Applied Social Research Methods Series, v.5, Sage Pubs., 2003.