

Legal Issues Related to Software Quality

Keynote at the 7ICSQ
October 8, 1997

Cem Kaner, J.D., Ph.D.

Legal Approaches

The Proceedings list several legal “theories” (ways you can be sued). I’ll skip most of them here (no time). But let’s distinguish:

- ***Negligence theories:*** *focus on public safety and public reliance on expert services. We look at the product and the process involved in creating the product.*
- ***Contract theories:*** *focus on living up to an agreement and on the quality and acceptability of the product or service as delivered. Process is irrelevant unless you contract to follow a process.*

Who are you?

- **How many of you are at this conference for the first time?**
- **How many of you are at your first testing or QA conference?**
- **How many of you have less than a year of software QA or testing experience?**
- **How many of you make packaged software?**
- **How many of you make custom software?**
- **How many sell products for less than \$1000?**
- **Can your products injure people?**
- **Is your primary focus on development of software for in-house use or for external use?**
- **How many are consultants rather than staff?**
- **Is software your company's primary business?**
- **How many of you believe that software quality engineering is a profession that should be licensed and regulated by the government?**

Source Materials

- www.kaner.com
 - software quality, development, and consulting
- www.badsoftware.com
 - law of software quality, consumer protection
 - my next book, *Bad Software: A Consumer Protection Guide*
- badsoftware.com is a new site, and I'm still in transition. These slides, and my course slides from 1997 Software Quality Week will be up on badsoftware.com by the end of the week. The Quality Week slides are on kaner.com now and will be there until November 1, 1997.

Legal Issues

Negligence

Quality/Cost Thinking Brings Benefits Even Without Heavy Measurement

I use it to win key battles--

Find the manager whose department will lose money because of a defect and bring her to the meeting that reviews the defect.

There are many internal failure costs. I don't suggest extensively measuring them. (I treat bad quality more as an executive or company-wide failure of commitment, and less as failure of measurement.) BUT the more you understand the range of failure costs, the more scope you have in bringing organizational pressure to bear on people and groups whose work is insufficient.

There are Risks

It is too easy to focus on easy-to-measure failure costs, such as Technical Support costs:

- **Lost sales from repeat-potential customers probably cost much more than tech support costs but we often ignore them because they are hard to measure.**
- **Many companies now charge \$3 per support-minute to recoup their external failure costs. Your numbers might look better, but is your business at risk?**

There are Risks

Quality/Cost analysis teaches the company to focus on its own costs, to minimize the sum of quality-related costs that are paid by the company.

What about the quality-related costs that are paid by the customer?

Remember the Pinto

- External Failure Costs = \$49.5 million
 - **180 burn deaths** \$200,000 each
 - **180 serious burn injuries** \$67,000 each
 - **2100 burned vehicles** \$700 each
- Total Costs to Repair = \$137 million
 - **\$11 per vehicle**

External failure costs are cheaper than repair, therefore ship it. Right?

Quality-Related Litigation: We Risk Being Blind-Sided

- **Whenever a defect in your product causes substantial losses to a customer, the customer has good reason to want to transfer those losses back to you. This is the foundation and point of quality-related litigation:
It's your defect; your customer says you should pay for it, not him.**
- *If you don't estimate the extent of the problems you are about to give to your customers, you risk being blindsided by unexpectedly expensive litigation.*

But what does this have to do with Negligence?

- *Cost-of-Quality analysis* balances prevention, appraisal and internal failure costs (including cost to repair) against the *seller's* external failure cost.
- *Negligence analysis* balances the company's prevention, appraisal, and internal failure costs (*especially costs associated with fixing the product*) against *society's* external failure cost.

Negligence Law & Cost-Benefit Analysis

“Negligence” always involves a tradeoff -- conduct must be *unreasonable*, not just harmful.

Duty:

- *products must not create unreasonable risk of injury or property damage***
 - *professionals must provide services at a level that would be provided by a reasonable member of the profession in this community***
- Breach**
 - Causation**
 - Damages**

Negligence Law & Cost-Benefit Analysis

Judge Learned Hand presented the tradeoff as a formula, in the famous case of the United States v. Carroll Towing Co.:

- Let B be the burden (expense) of preventing a potential accident**
- Let L be the severity of the loss if the accident occurs**
- Let P be the probability of the accident**

Failure to attempt to prevent a potential accident is unreasonable if $B < P \times L$.

Were You Negligent?

Factors that a Court Might Consider

1 Actual knowledge of the problem

No one likes harm caused by known defects.

2 Safety committee & hazard analysis

The wrong answer is, “Safety committee? What safety committee?”

3 Design for error handling

The law expects safety under conditions of foreseeable misuse. 90% of industrial accidents are caused by “user errors.” Deal with it.

4 Handling of customer complaints

Jurors will sympathize with mistreated customers.

Were You Negligent? Factors that a Court Might Consider

5 Actual testing coverage

But there are so many different types of coverage. Using judgment is more important than slavishly achieving 100% on one type of coverage.

6 Industry standards

- *In negligence, failure to follow a standard is relevant if and only if plaintiff can show that this failure caused the harm.*
- *To what extent should industry standards determine a standard of care?*
- *Are standards that are suitable for Mil Spec also suitable for shrink-wrap product development?*

Were You Negligent? Factors that a Court Might Consider

- 7 Are you using a consistent methodology?**
If not, how do you make tradeoffs?
- 8 Bug tracking methodology**
Do you have one?
- 9 Actual intensity / depth / breadth of testing.**
Did you make a serious effort to find errors?
- 10 Test plan: care in development and use of it.**
Why create it if you won't follow it?
- 11 Documentation**
- 12 Expertise of the staff**

Legal Issues

Professional Negligence

Professional Negligence

- I wrote about this in the proceedings, but my practice runs through the slides says we don't have time.
- Check www.kaner.com for:
 - **Computer Malpractice**
 - becoming “professionals” creates some risks
 - calling ourselves “professionals” (“Engineers”) creates additional risks
 - **Software Negligence & Testing Coverage**
 - a few criticisms of the CSQE process and result
- If we have time at the end, I'm glad to talk about this.

Legal Issues

Contracts

Uniform Commercial Code

- Governs all contracts for the sale of goods in the USA
- Treats sale of packaged software as a sale of goods.
- Treats sale of custom software as a sale of services, not covered by the UCC.
- This law is maintained and updated by the National Conference of Commissioners on Uniform State Laws (NCCUSL) a legal drafting organization funded by the 50 US states that writes all “Uniform” laws.
- The UCC is co-maintained by the American Law Institute, another non-profit body of senior lawyers.

Uniform Commercial Code Article 2B

- **UCC Sales are governed by Article 2, the Law of Sales.**
- **The UCC is being revised to include a new Article, 2B, the law of licensing of information. It will cover all software-related contracts (goods & services) and many other information-related contracts.**
- **This work started in the American Bar Association, 11 years ago. It became a NCCUSL project around 1992. It crystallized as the Article 2B project in 1995. To this point there was almost no customer-side advocacy. I started attending these meetings at the second 2B meeting, in February, 1996.**

Uniform Commercial Code

- **2B is scheduled for completion this spring, and introduction into state legislatures in fall, 1998.**
- **Last week, I sent a paper to the American Law Institute for their upcoming review of the 2B project (“Article 2B is fundamentally unfair to mass-market software customers”, coming soon to www.badsoftware.com). From that paper, here’s a list of some of the terms that can be imposed on customers in a mass-market license (shrink-wrap license that you don’t see until after the sale.)**

Article 2B Shrink-Wrap Terms

- **Disclaim all implied warranties, in a post-sale disclaimer.**
- **Limit licensor-provided remedies to replacement of the disk or to a partial or complete refund.**
- **Exclude incidentals and consequential damages even if they arose from a defect that the licensor knew about when the product was licensed to the customer.**
- ***No duty to attempt to cure (e.g. fix bugs).* (The licensor does have a duty to the non-mass-market licensee. But the mass-market customer has no such luck. The mass-market customer is stuck asking for damages, most of which will have been excluded under the contract.)**

Article 2B Shrink-Wrap Terms

- **Customers pay fee-based support from the first minute of possession of the product, even for actual defects in the product that are already known to the publisher. These calls often cost \$3 per minute, or \$20-\$150 per call or per incident.**

This practice is not new to 2B. It's happening today. But the legal status of the practice is unclear today, not blessed by a statute. 2B lets the unscrupulous publisher profit from its own defects and ensures that the customer has no recourse.

Article 2B Shrink-Wrap Terms

- ***Unlimited licensee-provided remedies:*** The licensee will be accountable to the licensor for consequential damages even though the licensor has excluded consequential damages to the licensee.
- ***Prohibit publishing detailed criticisms of the software.*** This is dressed up as a confidentiality restriction. Here are examples from current mass-market licenses, “You agree to hold the Package within your Organization and shall not, without our specific written consent . . . publish or communicate or disclose to third parties any part of the Package” (Symantec) and also “The customer will not publish reviews of the product without prior written consent from McAfee.”

Article 2B Shrink-Wrap Terms

- **Restrictions on the nature or purposes of use of the product.**
- **Restrictions against competition. For example, some mass-market products bar use that would result in creation of a competing product. This might seem to you to be harmless when it involves not using one compiler to create another compiler. But what about not using research material from an on-line service to write a book that would be published with a competing publisher? (This particular issue is real—it has arisen in private negotiations.)**
- **Restrictions on the location of use of the product, such as not being able to load or run a single copy on a machine that is used as a network server.**

Article 2B Shrink-Wrap Terms

- **Restrictions on who can use the product. (The neighbour's kids can't come to your house to play with your child's program.)**
- **Prohibition against reverse engineering.**
- **Prohibition against decompiling the software..**
- **Prohibition (via the ban of reverse engineering) against developing products that are interoperable with this one.**
- **Prohibition against lending the software.**

Article 2B Shrink-Wrap Terms

- ***Choice of law*** (entirely unrestricted to whatever state or country the publisher chooses)
- ***Choice of forum*** (entirely unrestricted for mass-market and commercial customers. Almost unrestricted for consumers.) A California publisher can restrict California customers a distant, non-American forum.
- ***Reduced statute of limitations, without tolling*** the statute while the publisher tries to fix the problems.

Article 2B Shrink-Wrap Terms: Progress Last Week

- **Override negotiated terms of the agreement.** *(This was probably dropped in the September Drafting Committee meeting. As I understand the Committee's motion, the next draft will neither authorize nor forbid such a term.)*
- **Include refusal terms, terms that even the seller knows would cause a reasonable customer who knew of the term to reject the entire transaction.** *(This will be transformed in the next draft. Terms that are unconscionable will be excluded. Refusal terms that are not unconscionable will not be excluded. The customer will accept or reject the agreement as a whole.)*
- **No reimbursement for incidental expenses associated with rejecting a license.** *(will probably change in the next draft.)*
- **Virtual elimination of licensor liability for viruses, even for a virus that the licensor knows or reasonably should know is on the disk.** *(Decided to delete 2B-311. Virus liability will be covered under merchantability and, some states, negligence.)*

What to do about 2B

- Attend the meetings. Next one is in Memphis, Peabody Hotel, November 21-23.
- Write your state legislator.
- Encourage professional societies to get involved in this legislation. 2B is one of several quality-related bills.
 - **Digital signatures**
 - **Intellectual property laws (e.g. reverse engineering)**

A Few Simple Ways to Reduce Litigation Risk

- 1 Look for ways that the product could cause injuries or property damage.**
- 2 Test your documentation.**
- 3 Test your marketing and sales collaterals.**
- 4 Don't lie to customers who call for support--deliberate post-sale misrepresentation is actionable.**
- 5 Don't charge in-warranty customers for calls to report bugs.**
- 6 Don't knowingly ship serious bugs.**
- 7 Don't keep shipping a product after discovering a critical bug.**
- 8 Treat customers sympathetically.**