Stanley A. Klein
7 Lorre Court
Rockville, MD 20852

Comment submitted to

Federal Trade Commission

regarding

High-Tech Warranty Project -- Comment, P994413

INTRODUCTION

1. To introduce myself, I am an independent consultant in computers, communications, and management science. I hold BS and MS degrees in Electrical Engineering and a D.Sc. In Operations Research. My consulting work is operated as a small, home-based business, organized as a single-member Limited Liability Company.

2. I am also a member of the Institute of Electrical and Electronics Engineers USA Committee on Communications and Information Policy. In that capacity, I followed the development of Uniform Commercial Code Article 2B and subsequently the Uniform Computer Information Transactions Act (UCITA). I participated in drafting of the IEEE-USA position on UCITA. As an individual, but drawing on information from IEEE and other sources, I testified at the Maryland hearing and participated in the public House and Senate worksessions held on the Maryland bill.

3. I also wrote an article on UCITA for the Monitor (publication of the Capital PC User Group), participated in a panel discussion of UCITA sponsored by the Internet Society, and made a presentation to CPCUG on "Protecting Yourself from UCITA". The article and presentation materials are attached as Appendices A and B.

4. As noted in Appendix B, I have made significant use of Draft 16 of Cem Kaner's paper "Software Engineering and UCITA" as a reference on UCITA's legal aspects. His book "Bad Software" (John Wiley, 1998, ISBN 0-471-31826-4) extensively discusses warranty issues. I also identified some issues on my own by examining the Maryland legislation and received other information as a member of the IEEE UCITA Task Force. I have included a copy of the final version of "Software Engineering and UCITA" (supplied to me by Dr. Kaner) as Appendix J to this document, although it is provided as a separate file in a separate format.

5. The issues in UCITA extend far beyond warranties and "consumers". UCITA is extremely tilted and carefully designed to advance the interests of large software publishers, "computer information" publishers, and on-line service providers and to strip away the rights and protections of everyone else. UCITA creates a legal minefield for anyone -- consumer or small business -- who can not afford the expensive legal and technical expertise to carefully evaluate the implications of click-wrap "agreements" and other UCITA-based contracts.

6. In some cases users will be bound by “agreements” that were “accepted” on their behalf without their knowledge or explicit approval by “electronic agents” embedded in the software. Furthermore, violation of these potentially abusive and incomprehensible “agreements” carries Federal criminal liability under the Federal “No Electronic Theft Act” and relevant court decisions.

7. The legal minefield created by UCITA also makes it very costly for individuals and small businesses to defend their rights, especially against the deep-pocketed interests that UCITA is designed to benefit. For example, it was pointed out in the Maryland worksessions that Accolade won the Sega vs. Accolade case thereby protecting their right (under Federal intellectual property law) to perform reverse engineering (an issue discussed below under UCITA-related use restrictions). However, the cost of winning the case bankrupted Accolade.

8. An individual recently reported on Slashdot (http://slashdot.org) that he had been sent a letter from a law firm demanding that he “cease and desist” from giving away some software he had developed to read the format of a bar code reader device that was being distributed for use with a catalog. The letter claimed that he has violated terms of some kind of shrinkwrap agreement included with the device. Even if he is completely within his legal rights (and many believe he is), the cost of defending his rights is clearly chilling.

9. UCITA was formulated and advanced in a process that was clearly unfair, biased, and unduly influenced by those whose special interests it would serve. The drafting committee chairman claimed in a Maryland hearing that UCITA reflected a compromise among numerous interests in an open, participatory process, and that the opponents were a few disgruntled participants who didn’t get *everything* they wanted in the compromise. UCITA almost speaks for itself as the product of a seriously biased process. Kaner describes the process as “progressively polarized and bitter”. Bitterness, polarization, and rejection of fair, reasonable proposals for change (of which there were many) are not characteristics of an open process focused on compromise. I also believe that the bill was deliberately drafted -- with so many overlapping provisions that strip away the rights of licensees and others -- to ensure that its abusive provisions could not be corrected by any set of simple amendments such as might be offered in state legislatures.

10. In addition, I either observed myself (e.g., from drafting committee material posted on the Internet), found in various documents, or learned in discussions with direct participants some indications that not only suggest the “openness” to have been a cynical charade but also give me serious doubts regarding the fundamental ethics of the process. I have attached Appendices C, D, E, and F to illustrate the information I considered in reaching this view. I strongly believe that the UCITA process calls into serious question the reputed integrity and ethics of the National Conference of Commissioners on Uniform State Laws and indicates a need for extensive reform.

11. The American Law Institute described UCITA (then called UCC Article 2B) as "a flawed approach to basic issues of contract law" and a "delegation of regulatory power to licensors who draft form [non-negotiable] contracts" (See Appendix G). Lawrence Lessig, in his book *Code and Other Laws of Cyberspace* (Basic Books, 1999, ISBN 0-465-03913-8) discusses UCITA in the context of issues that have serious implications for fundamental Constitutional rights.

12. Enactment of UCITA in Maryland was marked by a facade of serious consideration masking a process filled with political maneuvering and backroom deal-making. Important Maryland institutions that understood the dangers in the bill were politically muzzled. Most of the Maryland amendments were focused -- under pressure from the Attorney General -- on mitigating the provisions of UCITA that allow manufacturers of a wide range of consumer products to escape consumer protections. Other amendments were approved that purported to protect licensees' rights (e.g., under Federal copyright law) but were quickly recognized as ineffective by legal experts. At the end, the velvet gloves came off and the political ramrods came out. In my view, Maryland's enactment of UCITA was a demonstration of the insidious influence that can be exercised by deep-pocketed special interests.

13. At its core, UCITA is enabling legislation for abuse of customers and suppliers, where the "customer" includes not only consumers but small businesses, large businesses, government agencies, and anyone else who deals with the large software/computer-information publishers and on-line services. The provisions of UCITA should be viewed not only in the light of present technology but carefully considering what kinds of abuses might be legally enabled using future technology. I believe that some provisions of UCITA were included to facilitate customer abuse using technologies that were under development by its proponents but had not yet appeared or been recognized as existing in the marketplace. Some of these technologies have been reported and discussed since enactment of UCITA in Maryland (for example, technologies for interfering with backup and recovery and for violating privacy of word processing documents. In this respect I am fully in accord with the viewpoint expressed by Lessig -- that law must be considered in the light of relevant computer code.

SPECIFIC IMPACTS

14. The impacts of UCITA occur in four areas, but are closely intertwined among the areas. This makes the warranty aspects difficult to isolate. The areas are:

a. The scope of UCITA
b. The shopping and contracting process
c. Transfer and use restrictions
d. Warranties and related remedies
e. "Self help"

<u>The Scope of UCITA</u>

15. The scope of UCITA (as drafted by NCCUSL) creates serious concerns. UCITA covers "computer information", which includes anything processable by a computer. This scope includes software, information services, and on-line services. However, a "mixed transaction" which includes software as well as other goods can be "opted-in" to UCITA. The scope of "software" goes well beyond what people ordinarily think of as software. In fact, without software a computer (which is itself a good) has utility only as a paperweight or an art object. (a computer

chip itself is even often internally implemented by providing a processor much simpler than what can be externally observed, together with software that creates the chip's functionality.)

16. The question thus becomes: What is the scope of goods containing computers or other computer information? The answer is that an increasing number of products currently contain either computers or computer information, and that in a few decades it will be easier to approach the question by trying to list the products that don't contain computers or computer information. Some examples (either present or possible in the near future) include: automobiles, cameras, books, recordings, motion pictures, toasters, microwave ovens, heart pacemakers, electric lights, door locks, smoke detectors, furnaces, hot water heaters, coffeepots, television sets, faucet valves, and anything else of an electrical, mechanical, electro-mechanical, text, audio, or graphical nature. It is difficult to think of a list of products to exclude. For example, chemicals come to mind as not involving computers, but what if the packaging includes a computer-controlled mechanism for releasing measured quantities?

The Shopping and Contracting Process

17. In the shopping and contracting process, UCITA acts in many ways to ensure that the software publisher or on-line service provider has the upper-hand over customers, suppliers, potential competitors, and anyone else. The software publisher or on-line service provider is given iron-clad, fortress-like authority, while everyone else is placed on a slippery slope with weasel-worded "protections" that are designed to vanish like a desert mirage.

18. Begin with the fact that licensors are allowed to conceal their contract terms from the licensees until long after the transaction would ordinarily be regarded as having been concluded, i.e., to the point at which the licensee is preparing to install the program and begin using it. It required an *amendment* to the NCCUSL draft language (one of the few improvements made in Maryland) to ensure that the licensee has a right to print the contract terms for review prior to "manifesting assent" and a right to have a copy accessible for reference subsequent to "manifesting assent". I have been told that this issue was discussed in the drafting committee and that the software publishers fought inclusion of a similar requirement in the NCCUSL draft. NCCUSL adopted rules essentially allowing licensees to be forced to depend on licensors to tell them what terms they had accepted. If the licensee can be prevented from finding a copy of the accepted contract, the licensor has (yet another) way of changing the contract after the fact.

19. UCITA provides a number of ways for the software publisher or on-line service to unilaterally change the terms of contracts after acceptance by the licensee. These include merely posting the changes to a web site (continued use of the product after the posting would constitute acceptance of the changes), inclusion of changes in click-wrap terms to be accepted before loading bug fixes and program updates, and acceptance by a technician of click-wrap terms at initial installation time that override a previously negotiated agreement. If the user allows operation of an automatic Internet-based update feature in the software, the update feature could easily include an "electronic agent" programmed to automatically accept accompanying contract changes on the user's behalf.

20. In the process of comparison shopping and product selection, the licensee can not depend on publicly available information to determine the capability and quality of the product. Under UCITA, shoppers can be forced to depend exclusively on what the licensor tells them about the product. UCITA also provides licensors with means for evading treatment of their sales claims and product demonstrations as express warranties. UCITA grants control of shopping information to licensors by allowing them to impose use restrictions that can include prohibition of licensees disclosing or publishing information about product quality, performance, and other relevant product comparisons. One might imagine that this violates the principles of free speech, but the large software publishers have been treating this as a matter of trade secrecy and non-disclosure, which also has a legal basis. UCITA creates an extremely high barrier that must be overcome to escape use restrictions. (The restriction must be shown to violate a *fundamental* public policy the enforcement of which *clearly* outweighs enforcement of the restriction.)

21. UCITA allows the software publisher to retain ownership not only of the intellectual property but also of the software copy and the physical media received by the licensee. This takes away any user rights that are associated with "ownership" or "ownership of a copy" under relevant law.

22. UCITA includes a number of default provisions and other rules that can be used for abusing licensees and others. For example, there are at least two instances in which UCITA makes the plain language of a contract inoperable unless accompanied by other special language. These include a publisher's contract to correct defects and a contract for disclosure of an idea.

23. UCITA also contains a default provision allowing a software publisher to arbitrarily terminate almost any license after a "reasonable time" (for example, when the publisher decides to forcibly require the licensee to pay for upgrading to a new version of the software). This can be done even if the software license is purchased in a single payment (such as at a retail store) by simply including "source code" in the software package. UCITA does not define source code or state how much source code must be included to activate this provision. Note that the license for Windows 98 states that it contains source code -- notably a sample program for the software feature implicated in many of the recent information security scares of the past few years. (Maryland amended UCITA to require that any term limiting license duration be conspicuous. This is an example of the kind of pseudo-protective language frequently placed in UCITA both by the drafting committee and the Maryland amendments. Enforcement of a default provision does not require its rules to be stated in a contract term.)

24. The electronic commerce provisions of UCITA enable large, technically- and legally-sophisticated companies to engage in predatory and abusive business practices. One issue (discussed above) is the embedding of electronic agents in software preprogrammed by the software publisher to accept whatever contract terms or changes are proposed by the software publisher. Another issue (discussed below) is the ability to send important legal notices that the recipient is legally deemed to have received but which are formatted in such a manner that the recipient is unlikely to ever see them or be able to read them.

Use and Transfer Restrictions

25. UCITA allow a software (or other "computer information") publisher to impose any use or transfer restriction limited only by the creativity of the publisher's legal staff. As previously stated, UCITA creates an extremely high barrier to escaping such use and transfer restrictions.

26. Under UCITA, violation of a restriction can automatically terminate the license. Operation of software or use of information with a terminated license exposes the licensee to Federal criminal penalties. Each time software is started or information is used, it is copied internally within the user's computer. After a license is terminated, each internal copy operation is counted by applicable court decisions as a separate theft. When the cumulative value of thefts within a six month period reaches $1000, Federal law is violated. At $2500, it becomes a felony. For example, if a user discloses information to a prospective purchaser on defects or product performance of a $100 computer program (where prohibited by the license) and then uses the program every day for a month, the user can be prosecuted for a Federal felony.

27. One of the most serious software use restrictions commonly found is prohibition of reverse engineering -- the evaluation of software to discover its internal workings. Reverse engineering is a critical part of computer technology. Under Federal intellectual property law it is regarded as fair use and is explicitly allowed for certain purposes -- including interoperability, information security, and privacy protection -- under the Digital Millennium Copyright Act. UCITA essentially allows a non-negotiable contract to be created that waives these protections.

28. The technical implications of a reverse engineering restriction are far-reaching and extremely serious. Although UCITA recognizes that the licensee's data belongs to the licensee, if the data is stored in the licensor's proprietary format, the licensee's access to the data can be effectively blocked by termination of the license. Allowing restriction of reverse engineering stifles competition by preventing the creation and offering of products that can read the licensor's formats or otherwise interoperate with the licensor's products. This effectively allows the licensor to prevent a licensee from escaping the licensor's product (or to make escape very difficult and expensive), even if the product is defective or no longer satisfies the licensee's needs. Note that both the Sega vs. Accolade case and the bar code reader situation discussed above involve reverse engineering. The issue of reverse engineering has also been a major issue in some recent, highly publicized cases, such as the DeCSS case.

29. UCITA's provisions allowing software publishers to restrict reverse engineering also threaten to ultimately suppress the development of non-proprietary software, such as GNU/Linux, FreeBSD, Apache, Samba, and other low cost systems that are widely used and run about one-third to one-half of Internet providers and e-commerce sites. Reverse engineering has been an important part of the development process for all of these non-proprietary software systems, including its use in making them compatible with proprietary software and devices. Also, there is serious concern that the warranty provisions of UCITA (even as amended in Maryland) place the legally-unsophisticated, volunteer developers of non-proprietary software at financial risk.

30. UCITA contains no protections for licensee privacy. a simple extension of the theory that the publisher owns the software and can restrict its use leads to the concept that the publisher can inspect the use of the software to enforce the license terms. This would imply that the publisher can embed technology in the software that reports back to the publisher regarding relevant aspects of the software's use. For example, one restriction currently found in a license forbids the use of the supplied clip art to create any document that is scandalous or disparaging (with choice of law being that of Ireland). Enforcement of such restrictions could easily lead to intrusive violations of privacy, which have recently been reported as feasible with certain products.

Warranties

31. The warranty provisions of UCITA allow large, legally-sophisticated software publishers to substantially escape liability for defects, evade express warranties, impede customers seeking to protect their rights, and place at significant financial risk any legally-unsophisticated small businesses who perform services such as evaluating, recommending, installing, and maintaining software. UCITA allows the publisher to escape liability for, and even charge a fee for reporting, a defect known to the publisher, undisclosed to the licensee, and planned to remain unfixed. Under UCITA a small, legally-unsophisticated business that recommends the product of a large software publisher can be forced to shoulder defect liability that the large software publisher knows how to escape. The financial risk could ultimately force small computer services companies out of business and restrict market entry to large, legally-sophisticated companies.

Self Help

32. The self-help provisions of UCITA create a potentially serious threat to the information security of licensees' computer systems, some of which may be part of the national critical infrastructure. UCITA allows the licensor to intrude on the licensee's system and remotely disable their software if the licensor believes the licensee has violated the license terms. This means that if the licensee should publish a prohibited review of the software, disclose other defect or performance information prohibited by the license, financially reorganize without the licensor's permission (see Appendix a for a relevant license term), or use the software in a manner or for a purpose prohibited by the license, the licensor has the right to remotely disable the software.

33. UCITA provides a few legal protections for the licensee. There must be an extra click-wrap term separately accepted, and the licensee is entitled to prior notice. Maryland amended the NCCUSL version to prohibit use of self help on "mass-market" software, and I have heard that NCCUSL recently adopted a similar amendment. According to a column by Ed Foster in Infoworld (Appendix H), the definition of "mass market" does not necessarily protect business users or include software obtained in business-to-business venues. Note that the definition of a "consumer" is also drawn very narrowly -- a schoolteacher's use of a home Internet connection to look for information to use in class would probably be considered a business use under UCITA. Also, in a recent column (Appendix I), Ed Foster reported that the provision of UCITA allowing "electronic regulation of performance" appears to include an additional variation of self help.

34. To enable a publisher to exercise self help, information security holes must be embedded in the product that permit the publisher to intrude. However, the danger posed by UCITA self help is independent of the legalities of its exercise. All users will receive a product with the security holes, unless the publisher creates a separate version for delivery where self help can not be exercised. In addition, it is clear that if a user can restore the product from backup or reinstall it from original media, the effects of a self-help intrusion will be a temporary nuisance. Therefore, the publisher must design the product to interfere with the user's ability to perform backup and recovery, so once the product is "killed" it stays "dead".

35. The critical problem is that use of the security holes is not limited to the publisher. Anyone who discovers how to use them can perform a Denial of Service attack on the licensee (for that is what self-help is called in information security terms) and may be able to gain entry for other malicious purposes. Under UCITA's warranty provisions, the software publisher can completely escape liability for malicious third-party intrusion that exploits the self-help features. Also, innocent third-parties harmed by a licensor's improper use of self-help are not allowed to sue the licensor whose action harmed them.

36. One of the most important legal notices that can be sent under UCITA is a notice that the software publisher intends to exercise self-help. However, under the e-commerce provisions of UCITA, a notice is deemed "received" when it enters the recipient's Internet Service Provider even if no person ever sees it. UCITA contains no requirement that the recipient be able to process and read the notice. It only implies that the notice be processable by a "reasonably configured" system, which could be interpreted to require software that the licensee does not possess, has chosen not to install, or has chosen not to activate through option selections. It is entirely possible that the software could be designed to prevent the licensee from reading legal notices unless some undesired feature were installed or activated, such as one that opened an additional security hole or removed a privacy protection.

37. Furthermore, the notice is deemed "received" even if it is deliberately formatted to be intercepted and dumped by the filters that might be used by the recipient to intercept unwanted commercial e-mail (so-called "spam"). Such formatting is very simple. For example, under the default rules of the Microsoft Outlook spam filter (as reported on the Risks Forum), a message containing a double exclamation point, a dollar sign, and ",000" anywhere in the text will be treated as spam. It is easy to construct a reasonable-appearing legal notice that contains these elements.

38. Another example (due to Kaner) is that the licensor could choose to send the legal notice using an Internet Service Provider widely known as a source of spam. Many filtering systems are designed to recognize the addresses of such ISP's and reject messages from those addresses at a higher level than the individual recipient's desktop.

PROTECTING THE PUBLIC

39. One might ask whether the potential perils of UCITA will ever happen, given the pressures of a competitive market. In my view they are beginning to happen already, and UCITA's primary role is to give them ironclad legality. I also suspect that the stock valuations of some of the large software publishers and on-line services may have been bid so high that the implied investor expectations can not be met by ordinary business practices. Some of these companies will turn to customer abuse as a means of "making the numbers" expected by their investors. UCITA not only enables these companies to abuse their customers, but also enables them to deter their customers from escaping the abuse (e.g., by locking their customers into proprietary formats and preventing reverse engineering of those formats).

40. In my CPCUG speech (Appendix B) I stated that the best protection against the perils of UCITA is to avoid proprietary software as much as possible. If that can't be done, avoid proprietary formats. Beware conflict of interest by providers of electronic agents, and beware any embedded software that might function as an electronic agent. Do not engage in electronic commerce involving computer information, except under carefully limited circumstances with written back-up of all important notices wherever possible.

41. Non proprietary software (so-called open-source, free software, or open code) does not contain odious transfer or use restrictions that can result in Federal criminal penalties if they are violated. Non-proprietary software does not contain security holes placed there for purposes of enabling self-help. Non-proprietary software has warranty and damages disclaimers similar to those found in proprietary software, but non-proprietary software leaves the user in much better position than does proprietary software. Although the demands for expertise and support are currently somewhat greater with non-proprietary software, the quality and reliability are at least equal to that of proprietary software.

42. With non-proprietary software, if all else fails, the user has access to the source code. In principle, this allows anyone to identify the cause of a problem and either fix the problem or develop a workaround. The development status, bug lists, and future plans for non-proprietary software are often posted on the Internet, so at least the user can be fully informed. With proprietary software, many large businesses use "software escrow" (contingent access to the source code) as protection against the proprietary publisher going out of business, dropping the product, or failing to provide support. For non-proprietary software, software escrow is not only unnecessary, but its equivalent protections are available to consumers and small businesses.

43. Federal Government policy in the era of UCITA should be focused in two areas: (1) blocking the odious impacts of UCITA (which include most of its provisions and which continue to be identified), and (2) legally accommodating (or at least not inhibiting) the open-source software movement. The latter involves recognizing the movement's legal and organizational structures, such as the various open-source software licenses (see http://www.opensource.org), the voluntary, Internet-community-based methods by which non-proprietary products are developed, and the business models by which businesses in the movement generate revenue.

44. One example of legal accommodation would be to allow competitors in software-dependent industries (such as banking, electric power, insurance, or retailing) to cooperate in the voluntary, publicly-visible, Internet-coordinated development of open-source, industry-specific software or open, industry-specific data format standards without fearing anti-trust implications.

45. One component of open-source organizational structure requiring careful analysis is the role of non-proprietary software distributors. Some distributors add value to free software by selecting and aggregating software and offering warranties, support services, and documentation. Others offer the primary service of saving users connection time and difficulty by downloading and aggregating the software in convenient CD-ROM format.

46. One difficulty in regulating warranties is that provisions intended to prevent abuse by proprietary software publishers can have adverse effects when applied to non-proprietary software. a Maryland amendment allows free software to escape implied warranties, as long as it is not bundled with other goods, services, or non-free software. However, the CD-ROM itself may be considered a good and expose the distributor (as well as the volunteer developers of the software) to the implied warranty and relevant damages provisions. All open-source licenses have disclaimed implied warranties and related damages since their inception many years ago. Much software has already been produced and distributed under these licenses, and continues to be incorporated and modified in newly developed software that is also released under these licenses. There is significant concern regarding how to maintain the warranty and damages disclaimers to continue protecting volunteer software developers in the changed legal situation.

SCOPE AND PARTICIPATION IN FORUM

47. When UCITA becomes effective in Maryland on October 1, it becomes effective nationwide through its “choice of law” provisions (except in Iowa which has blocked it for one year). Given the extensive intertwining of the warranty issues with the other provisions of UCITA, the Commission’s initial public forum should focus on the broad range of UCITA-related issues, including those related to competition and business use of software. Included among the interests that should be represented are the professional societies in computers and software (such as IEEE), the open source movement, universities, libraries, consumer organizations, business users of computer software, authorities cognizant over critical infrastructure protection issues, independent software consultants, and experts in cyberlaw and related technical matters.

Appendices

a. S. a. Klein, "UCITA - a Proposed Law You Need to Know About", text as submitted for the March 2000 issue of The Monitor, publication of the Capital PC User Group

B. S. a. Klein, "Protecting yourself from UCITA", presentation materials for the CPCUG meeting of July 10, 2000 (Also posted at http://

C. Ed Foster, "Observations on the UCITA drafting process", downloaded from http://www.infoworld.com/ucita

D. Selected Portions of a Letter of the Society for Information Management to the UCC 2B Drafting Committee. Only the portions of the letter related to drafting process issues have been included.

E. Memorandum from former American Law Institute Article 2B drafting committee members declining participation in UCITA drafting committee

F. Cem Kaner, "Why You Should Oppose UCITA"

G. Braucher-Linzer Motion presented to the American Law Institute. [The ALI adoption of this motion and the failure of the drafting committee to comply caused ALI to drop out of the UCC Article 2B drafting process and the project's renaming by NCCUSL as UCITA.]

H. Ed Foster's Gripe Line column of April 21, 2000. The column appeared in Infoworld. The text presented here was downloaded from http://www.infoworld.com

I. Ed Foster's Gripe Line column of August 25, 2000. The column appeared in Infoworld. The text presented here was downloaded from http://www.infoworld.com

J. Cem Kaner, "Software Engineering and UCITA". This paper was initially published in the *Journal of Computer and Information Law*, Vol. 18, #2, Winter 1999/2000, and is provided as a separate file.

Appendix a

UCITA - a Proposed Law You Need to Know About

By Stanley a. Klein

(Submitted for the March 2000 issue of The Monitor, publication of the Capital PC User Group)

a bill is being considered by the Maryland legislature and appears to be on its way to passage by the Virginia legislature that affects every computer user, every software developer, and possibly every consumer. It has been controversial on the Internet and the trade press and has begun to hit the daily papers. The bill is called the Uniform Computer Information Transactions Act (UCITA). It was prepared in a controversial process by the National Council of Commissioners on Uniform State Laws (NCCUSL).

CPCUG doesn't take positions on legislation, but it is very important for CPCUG members to become informed about UCITA and to take their own positions. In the interests of disclosure, the position of the author is one of opposition, based on about three years of following the proposed legislation for the Institute of Electrical and Electronics Engineers (IEEE) USA Committee on Communications and Information Policy. Although the author is a non-lawyer, the effort included liaison with the IEEE-USA Intellectual Property Committee, which followed the legislation for 10 years and includes a number of lawyers expert in the relevant issues.

UCITA started out as a draft update to the Uniform Commercial Code (UCC), a joint project of NCCUSL and the American Law Institute. The UCC is a law, adopted individually in each state based on wording provided by NCCUSL. UCC Article 2 governs contracts for goods and services. The UCC establishes default contract provisions (for example, if there is no written contract) and places limits on certain types of contract provisions (such as standard form contracts presented to consumers). UCITA started out as a draft UCC Article 2B. Controversy over both the draft and the drafting process became so great that the American Law Institute dropped out of the project, preventing it from becoming part of the UCC. NCCUSL changed the name, adopted the draft on its own and sent it to the states for enactment.

Currently, many provisions of the shrink wrap and click-through agreements that come with computer software and on-line services have been held by courts to be unenforceable. The reasons relate to requirements of UCC Article 2 -- which is the current governing law for these types of contracts -- and to the provisions of Federal intellectual property law. For example, UCC Article 2 doesn't allow sellers to change the terms and conditions of a sale after the sale has been completed. Some courts have interpreted the shrink-wrap agreements as doing just that.

Another example is that Federal intellectual property law contains provisions regarding users' rights that the shrink-wrap agreements attempt to negate. These include such "fair use" rights as the right to resell the copy the user purchased and the right to reverse-engineer the software for specific purposes. The issue surrounding fair use of published information is not new. In the late 1800's and early 1900's book publishers tried to "license" the information in their books to restrict ways the information in the book could be used by the reader and to control the market for second-hand books. Their efforts were rejected.

In addition to effects on users' rights, UCITA affects the responsibility of software publishers for the quality of their software. According to many organizations, including the Institute of Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery, and the Software Engineering Institute, UCITA would relieve software publishers of any responsibility for software quality.

Beyond software, UCITA covers contracts for information services and electronic contracting for both software and information services. There is a parallel bill, the Uniform Electronic Transactions Act (UETA) that is not controversial and covers electronic commerce generally, except for contracts covered by UCITA if the latter is adopted. UCITA contains many controversial provisions that were deleted from UETA. One example is that while UETA requires an electronic record to be sent in a form capable of being processed by the recipient's software, UCITA requires only that the record be sent in a form capable of being processed by "reasonably configured" software. Also, while UETA requires that notices be sent to the recipient, UCITA allows contract terms to be changed by posting the new terms to a web page. Continued use after the posting could be treated as user acceptance of the new terms.

To understand the workings of UCITA, it is necessary to also understand the provisions of the shrink-wrap agreements that UCITA would make enforceable and the fair-use provisions of Federal copyright law that UCITA would undermine. Most people don't read the shrink-wrap agreements in detail while they are installing their software. They just click "I Accept". Some of the terms they may be accepting include:

- "You may not translate, reverse engineer, decompile, or disassemble the Product except to the extent the foregoing restriction is expressly prohibited by applicable law."

  If this provision were made enforceable, it could negate any user rights under both fair-use court decisions and the Digital Millennium Copyright Act (DMCA), adopted by Congress about a year ago. Under the DMCA, a user has the right to break encryption-protected access management controls to reverse engineer the software for a number of purposes, including :

  -- Discovering software elements such as interfaces and file formats to enable creation of compatible (interoperable) products.

  -- Performing encryption research

  -- Testing a system for information security

  -- Determining if the software is collecting and disseminating personal information without disclosure to the user.

  However, the DMCA doesn't expressly prohibit contractual restrictions on reverse engineering. For example, under UCITA, it could become legally difficult to create programs capable of importing other programs proprietary file formats without permission of the other publisher. The effect could be to create a high barrier to users who want to switch from one word processing or accounting program to another.

- "Neither this Agreement, nor any rights hereunder, may be assigned by operation of law or otherwise, in whole in part, by Client without the prior, written permission of [the software provider].. Any sale of more than fifty percent (50%) of the common voting stock of, or other right to control, Client shall be deemed an assignment. Any purported assignment without such permission shall be void."

  If a clause like this were made enforceable, a business would be stupid to allow a technician to install software. A prudent business would require that the CEO and the Corporate Counsel personally participate in each installation of new software and that employees be strictly prohibited from installing any other software on company computers.

The proponents of UCITA claim that a business would buy a site license that could be separately negotiated to avoid this type of clause. However, according to a white paper on UCITA by Principal Financial Group, about half of the software acquired by even large companies is in the form of single copies purchased from retail stores. In addition to presenting a problem to regular businesses, this type of clause could put second-hand software stores out of business and prevent people from selling their old software packages at yard sales and swap meets.

You may wonder how license provisions like this could be enforced by the publisher. UCITA allows something called "self help" under which the publisher is permitted to break into the user's system and remotely disable the software. There are a few legalities the publisher must observe. These include a second "I Accept" click on a clause allowing self help, and an e-mail notification 15 days before the break-in (to give the user time to convince a court to stop the break-in). Of course, the functionality that the publisher builds into the software to support the denial-of-service attack is also available to anyone who learns about it and might want to launch it, such as a disgruntled employee or a hobbyist intruder who wants bragging rights. The attack could also be triggered by a software bug.

! "No Warranties. [The publisher] expressly disclaims any warranty for the Software Product. The Software product and any related documentation is provided "as is" without warranty or condition of any kind, either express or implied, including, without limitation, the implied warranties and conditions of merchantability, fitness for a particular purpose, or noninfringement. The entire risk arising out of use or performance of the software product remains with you." [A subsequent provision disclaims any liability for damages, "including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss".]

This particular publisher puts all risk on the user, including the risk of the *publisher's* having infringed someone else's copyright, patent, or trademark. According to IEEE, this even includes defects the publisher knew about at the time of sale, did not disclose to the purchaser, and knew could have serious financial impacts on the purchaser.

! "The customer shall not disclose the results of any benchmark test to any third party without [the publisher's] prior written approval. The customers will not publish reviews of the product without prior consent from [the publisher]."

Although UCITA allows contract clauses to be thrown out if they are "unconscionable" or "against fundamental public policy", nondisclosure clauses are common in many types of contracts. It could take years of expensive litigation to find out if courts would be willing to throw out these clauses.

Also, the previous example puts all the risk of using the product on the user. These clauses prevent users from finding out from each other that the product has defects. UCITA would legalize both sets of clauses, which together create an open invitation for publishers to rush buggy software to market, knowing that they could do so without any responsibility for the consequences.

These examples are just a few of the many impacts of UCITA. The list of URL's given in Table 1 provide many more. CPCUG members should familiarize themselves with this proposed legislation and make their

views known to those responsible for considering the bills. Contact information for Maryland legislators can be found at http://mlis.state.md.us and for Virginia legislators at http://legis.state.va.us.

Table 1. Sources of Additional Information on UCITA
(Prepared 2/27/2000 by S. A. Klein)

General information

Site	Description
http://www.4cite.org	A coalition of organizations opposing adoption of UCITA
http://www.badsoftware.com	Includes or links to numerous opposition comments
http://www.2bguide.com	Includes both pro and con comments. "Whatsnew" page has extensive links to relevant UCITA and UCC-2B documents
http://www.ieeeusa.org/grassroots/ucita	IEEE-USA "Grassroots" web site provides links to numerous documents including NCCUSL materials and relevant IEEE-USA letters and positions

Specific documents

Document	URL
July 1999 IEEE-USA letter to NCCUSL opposing UCITA	http://www.ieeeusa.org/forum/POLICY/1999/99july20.html
Memo by Steven Chow, dissenting member of UCITA drafting committee	http://www.2bguide.com/docs/citopp.html
Letter by FTC staff to NCCUSL opposing UCITA	http://www.ftc.gov/be/v990010.htm
Memo describing adverse impacts of UCITA on businesses (Prepared by Principal Financial Group)	http://www.4cite.org/prinlng.html
Memo from former ALI members of drafting committee declining further participation in UCITA	http://www.2bguide.com/docs/50799dad.html
Letter to NCCUSL from President of Association for Computing Machinery opposing UCITA	http://www.acm.org/usacm/copyright/usacm-ucita.html
IEEE-USA position statement on UCITA (approved February 2000)	http://www.ieeeusa.org/forum/POSITIONS/ucita.html

---

Stanley A. Klein is a consultant in computers, communications, and maamgement science with a focus on technical issues analysis in information security, computer project risk assessment, and a variety of other areas. He holds BS and MS degrees in Electrical Engineering and a D.Sc. in Operations Research. He is Principal Consultant of Stan Klein Associates, LLC, and can be reached at sklein@cpcug.org or by phone at (301) 881-4087

Appendix B

"Protecting Yourself from UCITA"
Overhead slide presentation text from speech given on July 10, 2000 to a meeting of the Capital PC User Group

---

Protecting Yourself From UCITA
(The Uniform Computer Information Transactions Act)

Stanley A. Klein
Stan Klein Associates, LLC
(301) 881-4087
sklein@cpcug.org

Agenda

- **!** Scope and Background of UCITA
- **!** Overall Impacts of UCITA
- **!** Protection Strategies
  - Purchasing and contracting process
  - Avoiding proprietary lock-in
  - On-line contracting (UCITA-related)
  - Consultants and small developers (including Open Source)
  - Protection against "Self-Help"
  - Non-proprietary software (GNU/Linux, FreeBSD, etc.)
- **!** Current Status
- **!** Conclusions

Important Note

- **!** I am not a lawyer
- **!** See reference notes for legal information sources

Scope of UCITA

- **!** Transactions involving “computer information”
  - Software
  - On-line services
  - Any computer-processable information
    - Movies
    - Stock quotes
    - Reference information
    - Music
    - Books
  - Software in embedded computers (mixed transaction opt-in)
  - Associated documentation and packaging

Background of UCITA

- **!** Uniform Commercial Code
  - National Conference of Commissioners on Uniform State Laws (NCCUSL)
  - American Law Institute (ALI)
- **!** UCITA started as UCC Article 2B
- **!** Governs licenses and provides default rules
- **!** Process dominated by major software publishers and on-line services
- **!** ALI backed out and refused to participate further
- **!** NCCUSL renamed and sent to states
- **!** Heavy lobbying and deal-making by proponents

Overall Impacts of UCITA

- **!** Contracting
  - License terms can be concealed until installation
  - Variety of means for unilateral change by publisher or service provider
  - Click-wrap at installation can override negotiated agreement
  - Numerous rules and defaults outside normal expectations
  - License ends after “reasonable time” if source code included
  - Definition of “receipt” for e-mailed contract notices
  - Numerous legal pitfalls for consultants and small developers

- Violations that void licenses can easily become Federal criminal matters under “No Electronic Theft Act”

Overall Impacts of UCITA (continued)

- **!** Use and transfer
  - Wide range of restrictions and conditions allowed - anything the publisher's lawyer can invent
  - High legal barriers to escaping restrictions and conditions
  - Can override protections of Federal copyright law
  - Numerous ineffective "user-protective" provisions
  - Publishers can prohibit public criticism and benchmarking
  - Publishers can prohibit reverse engineering
  - Publishers can restrict transfer or resale
  - Publishers can restrict use of product for certain purposes
  - Tool providers can demand ownership of resulting products

---

Overall Impacts of UCITA (continued)

- **!** Defects, warranties, and remedies
  - Publishers can escape liability for defects and infringement
  - Numerous obstacles to customers pursuing damage claims
  - Software need not conform to demo or documentation
  - Purported bug fix can carry click-wrap waiving further recourse before fix is applied
- **!** "Self Help" remote intrusion and disablement
  - Requires additional click-wrap acceptance and prior notice
  - Publisher allowed to disable software remotely if they believe license has been violated (Denial of Service attack)
  - No liability for malicious use of self help capability by others

---

Protection Strategies - Purchasing and Contracting Process

- **!** Don't depend on getting information from reviews
- **!** Need to carefully review all fine print of "agreements"
- **!** Selection and comparison-shopping process should not end until after acceptance of license terms
- **!** Businesses need to mandate referring all "click wrap" screen contents for management and legal approval
- **!** Businesses need formal process for recording and managing licenses and approvals
- **!** Need to check often for web-posted contract changes

Protection Strategies - Avoiding proprietary lock-in

- **!** Proprietary lock-in can result from restriction of reverse engineering
  - Prevents or limits file format import/export or other interoperability with competing or non-partner products
- **!** Proprietary lock-in:
  - Makes it difficult to switch to a better product for your needs
  - Can be disastrous if you lose the right to read your own data
- **!** Beware proprietary file formats and network protocols
- **!** Unless you will never need to switch products:
  - Favor non-proprietary formats for storage and backup
  - Avoid proprietary extensions to standard formats/protocols

---

Protection Strategies - On-line contracting

- **!** Don't allow an "electronic agent" to "represent" you unless you are certain it will protect your interests
  - Beware conflict-of-interest by electronic agent providers
- **!** Contract notices are deemed "received" even if unreadable or dumped by spam/porn/virus filter
  - Beware dependence on e-mailed notices
  - Demand non-email redundant backup of e-mailed notices
  - If you must depend on e-mail, carefully redefine "receipt"
- **!** Example of spam filter rule from Microsoft Outlook:
  - Text contains "!!" and "$" and ",000" [from Risks 20.89x]

Protection Strategies - Consultants and small developers (incl Open Source)

- **!** Legal pitfalls require consultants to seek advice:
  - Consultants can be liable for what large publishers escape
  - Special rules for "disclosure of ideas"
  - Small developer can't put transfer restriction on large publisher
- **!** Concern regarding liability of Open Source (GNU/Linux-related) project participants
  - May need revision of Open Source licenses

- What to do about existing body of free GPL'ed software

Protection Strategies - Protection against "Self-Help"

- **!** Know that when you see "self-help" it means break-in and disablement (targeted Denial of Service attack)
- **!** Don't agree to it
- **!** Avoid purchasing software with built-in security faults that enable self help
- **!** Beware software with unusual or vendor-dependent backup/recovery
  - Successful self help requires interfering with recovery
  - Self help is a mere nuisance if user can reinstall from media and/or restore from backup without vendor involvement

---

Protection Strategies - Non-proprietary software (GNU/Linux, etc.)

- **!** Disadvantages:
  - Currently need greater technical expertise and/or support
  - Some device manufacturers don't support or cooperate
  - Popular applications tend to lag
- **!** Advantages:
  - Low acquisition cost and perpetual license
  - Development status is clear. Bugs are disclosed.
  - Source code available for maintenance and upgrade
  - Unrestricted use and transfer, except staying non-proprietary
  - No self-help or interference with backup/recovery
  - Specialized and research-based applications tend to lead

Current Status

- **!** Effective in Maryland: October 1, 2000
- **!** Effective in Virginia: July 1, 2001 after ongoing study

- Choice-of-law provision makes effective elsewhere
- Blocked in Iowa for residents and local businesses
- GSA working on policy response to perceived serious threat of self-help-capable software
- FTC has open inquiry on warranty issues - comments due September 11
- Proponents targeting DC and many additional states

Conclusions

- UCITA is severely tilted to benefit large software publishers and on-line services versus everyone else
- Need to take “agreements” seriously and study fine print
- Businesses need to carefully revise their procedures
- Need contingency plan for loss of right to read your files
- Need to beware self-help and self-help capability
- Need to beware UCITA-related on-line contracting
- Consultants need to address special legal problems
- Recommend considering non-proprietary software

Reference Notes

- Cem Kaner, “Software Engineering and UCITA”, Draft 16, Submitted to Computer Law Journal. To be posted: www.kaner.com or www.badsoftware.com
- http://www.infoworld.com, especially Ed Foster’s column.
- http://www.4cite.org
- http://www.ieeeusa.org/grassroots/ucita
- http://www.ucitanews.com
- Enrolled version of HB 19 on http://mlis.state.md.us/2000rs/billfile/hb0019.htm
- http://www.ftc.gov/os/2000/05/hightechforum.htm

Appendix C
Ed Foster, "Observations on the UCITA drafting process"
Downloaded from http://www.infoworld.com/ucita

Observations on the UCITA drafting process

By Ed Foster

People keep asking me the same questions -- how did a monstrosity like UCITA come to be? What is this obscure process that created it?

To even begin to explain how NCCUSL (the National Conference of Commissioners on Uniform State Laws) drafted and approved UCITA for submission to the state legislatures is a very daunting task, and doing so at this point may seem like crying over spilt milk. If UCITA is to be stopped in the states, however, it's going to be necessary for those who fight it to understand how flawed this process is. And as the only journalist to witness it up close over the last four years, I'm obliged to try to describe what I've seen.

NCCUSL is a group of 350-plus commissioners appointed by their respective states and charged with responsibility for drafting laws that can be adopted uniformly by all the states. The organization has a long and prestigious history, most notably the creation of the Uniform Commercial Code. (The Uniform Commercial Code was created facilitate the laws of interstate commerce) The commissioners are all highly respected individuals, and I have not encountered one whose personal integrity I would question.

Yet this is the group who took a software industry wish list and made it a model law that is supposed to be enacted throughout the nation. How is that possible? It's possible because NCCUSL is a stacked deck, one that by its very nature is most easily influenced by the large commercial interests whose mainline business is directly at stake. It's a game the consumer side just can't afford to play.

NCCUSL critics have pointed this out before in the context of other UCC articles and uniform laws, but I have to believe it was never so amply illustrated as in the UCITA/Article 2B drafting committee. (UCITA was previously called Article 2B) UCITA is the result of an effort that began more than ten years ago -- by the time the first representatives of consumer interests got to the table in early 1996 (or late 1995, if you count me and my readers), the basic principles of UCITA were already well entrenched in the draft. And each one of them will tell you today that their participation since has at best resulted in only minor improvements. In fact, many felt their participation was

counterproductive, as it allowed NCCUSL leadership to claim that consumers had meaningful representation in the drafting process.

Just to briefly summarize a few examples of why consumer advocates found their efforts to influence UCITA so futile, in the fall of 1998 Article 2B (as UCITA was then known) drafting committee officials were trumpeting a compromise on one particular issue which had been painstakingly worked out between one consumer advocate and one software company representative. The committee's crowing about this unprecedented development led some publications to state the compromise had been adopted. In fact, in its November, 1998 meeting the committee accepted those portions of compromise the consumer advocate had conceded, while totally rejecting those portions the software publisher had agreed to give in exchange.

At its one-day session just before the NCCUSL annual meeting that adopted UCITA in July, 1999, the UCITA committee was presented with proposed changes to the draft by the Recording Industry Association of America, one of the publishing groups that had been voicing strong opposition to UCITA over the past year. The RIAA openly stated they were willing to take a neutral stance on UCITA's enactment if their changes were adopted. Although members of the committee expressed ignorance of just what the RIAA's language actually meant, they did not even bother to get clarification before adopting it all. "The most important thing is the affected industry wants it, so I move we adopt it," one committee member stated.

Affected industries could generally get what they wanted from the UCITA/2B committee, but affected customers could not. This was also shown to be true of NCCUSL as a whole a few days later during its annual meeting in a surprising event that did not directly involve UCITA. Another NCCUSL drafting effort is a revision to the existing UCC Article II, the sale of goods law that has stood for half a century and is one of the primary reasons for NCCUSL's lofty reputation. Like UCITA, revised Article II was up for a final vote at the July meeting, and it appeared to be further along in the line-by-line debate of the draft than UCITA when the NCCUSL leadership announced they had decided to halt the debate and postpone a vote on Article II for at least another year.

It's difficult to convey how stunned the entire room was by this announcement. Even commissioners who were opposed to Article II expressed shock that the decision had been taken out of their hands by the NCCUSL leadership. Consumer advocates were considerably more distraught, because the Article II revision has been the focus of much of the lobbying efforts that Consumers Union and others could afford. Opponents, which included an imposing list of influential manufacturing associations, believed that the revised Article II draft was too

consumer-friendly. But the list of UCITA opponents -- which by the time of the UCITA included attorneys general of half the states -- was an even more imposing one. Yet the NCCUSL leadership chose to kill Article II while allowing the decidedly consumer-unfriendly UCITA to sail through.

The clearest demonstration of how NCCUSL is a stacked deck comes from an incident involving the UCITA drafting committee reporter. The very week after NCCUSL approved UCITA, Prof. Ray Nimmer, a University of Houston law professor who served as the UCITA and Article 2B drafting committee reporter throughout its existence, was called as an expert witnesses to testify for Microsoft in a little known federal case it was waging with the IRS over a disallowed tax deduction. As is common with expert witnesses, Nimmer charged Microsoft a fee for his time and expenses based on his standard legal consultant rates.

The reporter plays a unique and critical role in the NCCUSL process. He or she is the principal author of the law itself, under the direction of the drafting committee and the state commissioners as a whole. After the draft is approved for distribution to the state legislatures, the reporter writes the Reporters Comments, notes on individual sections of the law often used by judges to help interpret how it should be applied. Perhaps most important, reporters are the subject matter experts, usually hired by NCCUSL specifically because of their expertise in both the law and the current commercial practices the proposed law will cover.

Nimmer's expertise is unquestioned -- he is the author of the standard text on computer law. But his name may ring a bell with some longtime InfoWorld readers for another reason, and a handful of you have actually met him. Way back in the fall of 1995, when reader gripes about the "known bug" syndrome first got me involved in what then had just been renamed UCC Article 2B, Nimmer and I arranged several meetings with InfoWorld readers to try to get their feedback into the law. In a sense, he had a mandate to represent InfoWorld readers in the process, as well as others who didn't have a lawyer at the table.

When I started hearing rumors about Nimmer testifying for Microsoft, I found it hard to believe. Even after he readily acknowledged it to me, I remained somewhat shocked. Perhaps this is due to the journalist's perspective -- we sometimes get asked to be expert witnesses, too, but it would be a no-brainer for me that I couldn't take a fee from a company I might be writing about the next week. Shouldn't a NCCUSL reporter be held to the same ethical standards as the journalistic variety?

In Nimmer's own defense, he points out the issue on which he testified

for Microsoft was a fine point of software law history irrelevant to UCITA. If it wasn't Microsoft specifically, he says, probably no one would have perceived his testifying as an issue. And he and his defenders in the NCCUSL leadership argue that, since it is his field of expertise, to say he could have done no legal work for the last ten years for any software company would have been an extreme financial hardship.

Even so, shouldn't all participants in the UCITA process at least have been informed what Nimmer was doing? As it was, most participants including many UCITA committee members themselves were not aware of it when they met on July 22nd for their sole day of public input on UCITA. The commissioners who approved UCITA the next week after listening to Nimmer defend the draft in the debates were also not informed -- at least officially -- that he would be working for a company with a big stake in UCITA a few days later.

NCCUSL executive director Fred Miller says that Nimmer followed the one disclosure rule the organization has for reporters by clearing it with Miller in the spring when Nimmer was first asked to testify. Miller says he saw little reason to make a big deal out of it since the draft of the law was already close to final form and the issue in the Microsoft case was unrelated.

Let me make it clear that I'm certain Ray Nimmer was not influenced by this fee from Microsoft to do something he shouldn't, but that's not the point. The real issue here is the reluctance of NCCUSL's leadership even now to have these relationships openly disclosed. A fair and impartial process requires at least that much.

It is indeed hard for NCCUSL reporters, commissioners and officials to avoid having conflicts of interest -- most of them are commercial contract lawyers who have represented many different business clients through the years. And that's the ultimate conflict of interest in having this organization draft this law. There is, after all, only one interest group that will surely benefit from UCITA in the long run, and that's the lawyers who represent big companies.

Appendix D
Selected Portions of a Letter of the Society for Information Management
[The main part of the letter has been deleted. Only the process related portion is provided here.]

VIA FAX AND E-MAIL ATTACHMENT
Fax: 202-408-0640
ccring@ober.com

November 25, 1998

Carlyle C. Ring, Jr.
Chairman, NCCUSL Article 2B Drafting Committee
Ober, Kaler, Grimes & Shriver
1401 H. Street NW – 5th Floor
Washington, DC 20005

Re: Electronic self-help

Dear Connie:

At the November 1998 Drafting Committee meeting for UCC Article 2B, observers did not receive a copy of the electronic self-help provision proposed by Committee member Tom Grimshaw until minutes before the proposal was considered by the Committee. Licensee representatives were then criticized by the Committee (unfairly, we think) for being unwilling to take a position either endorsing or opposing the proposal without time for more careful review. Moreover, although SIM had followed procedures by submitting its own proposal for wording of the self-help provision by October 10 and making it available on the 2B Guide website for public review in advance of the meeting, SIM's proposal was not even mentioned at the meeting.

Several of us have now had an opportunity to review the self-help language adopted by the Committee and are prepared to give you our thoughts.

•
•
•

[NOTE: The letter goes on to discuss the SIM views and proposals in the area of self help. That part is not reproduced here.]

•
•
•

Our letter is restricted solely to comments on self-help. We expect to provide comments on other parts of the draft after the new draft is available for review.

We look forward to the Committee's consideration of our self-help proposal, and would ask that it be placed on the agenda for the February meeting.

Sincerely,

James R. Helms
Barney R. Kantar
Elaine M. McDonald
Paul M. Nelson
Susan H. Nycum
Randy J. Roth

Cc: National Conference of Commissioners on Uniform State Laws
American Law Institute
Ray Nimmer, Reporter

Appendix E
Memorandum from former ALI drafting committee members declining participation in UCITA drafting committee

Memo

To:	Uniform Computer Transactions Act Drafting Committee
From:	David Bartlett, Amy Boss, David Rice
Date:	May 7, 1999

The American Law Institute and the National Conference of Commissioners on Uniform State Laws have decided not to proceed with Article 2B as an addition to the Uniform Commercial Code. Instead, the Conference plans to bring forward the Uniform Computer Information Transaction Act as a proposed uniform state law. This change had the effect of ending our roles as ALI members of the Drafting Committee for Article 2B. Instead the Conference has asked that we serve as advisors to the UCITA Drafting Committee.

The three of us have been actively engaged members of the Drafting Committee for Article 2B since its inception, and were involved as well in the prior evolutionary stages of what became the UCC 2B draft. We believed, as did the American Law Institute in deciding to co-sponsor the project, that a focused effort to clarify contract law governing computer software and related transactions was desirable. We have enjoyed working with and learning from all of our NCCUSL colleagues while seeking to accomplish this. We greatly value the many new friends we have made through participation in this ambitious enterprise.

Those factors have made our individual decisions difficult. Nonetheless, the three of us have each concluded that we will not continue to participate as advisors. It is important to us, and we hope instructive to you, to share the reasons common to our decisions.

A few months ago, following the final Drafting Committee meeting, it became apparent that the Conference was determined to recommend the draft for final approval in July despite concerns from many sectors regarding its suitability for enactment. The three of us consequently recommended to the leadership of the Institute that the draft not be included in the UCC at this time. Our recommendation was based on a number of underlying concerns including matters of substance, process, and product.

In terms of product, the draft has, in attempting to address numerous concerns of affected constituencies, progressively moved away from articulating sufficient and generally applicable default rules toward establishing increasingly particular and detailed rules. In so doing, the draft sacrificed the flexibility necessary to accommodate continuing fast-paced changes in technology, distribution, and contracting. In terms of process, the guiding principle appeared to be the Conference's desire to expedite approval and commence enactment of the draft. This led to obviating rather than learning from strong concerns expressed by Conference and Institute discussions over the entire course of the project, ranging from scope and drafting to the interplay with intellectual property rules. Substantively, as you know, the three of us often disagree. Yet we believe that some rules, although they may assure important constituencies' support for the draft, nonetheless jeopardize enactability because of the ultimate balance of interests achieved.

These are not new, or newly expressed, concerns. They are fundamental concerns and have been aired before in Conference and Institute discussions, by individual members, Drafting Committee members and observers, and Internet discussion list participants, as well as by software and other computer science enterprises and professional organizations, law professors, and editorial writers. The persistent din of these concerns has contributed significantly to our decision to decline the invitation to participate as advisors.

The limited time remaining before presentation of UCITA for final approval does not permit changes that might address such fundamental concerns. Thus, inasmuch as the draft is now on the final approval track, what contributions we could make to the draft have been made.

We therefore decline the Conference's invitation that we participate as advisors.

Appendix F

Cem Kaner, "Why You Should Oppose UCITA"

[Received from the author by e-mail. The final section entitled "In Closing" contains additional information regarding the biased nature of the drafting process.]

CEM KANER, J.D., Ph.D.

Law Office of Cem Kaner		**kaner@kaner.com**
P.O. Box 1200		**408-244-7000 (Voice)**
Santa Clara, CA 95052	**www.badsoftware.com**	**408-244-2181 (Fax)**

Why You Should Oppose UCITA

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

The Uniform Computer Information Transactions Act (UCITA) is being actively considered in several states and might soon become law in some of them. I am one of the bill's critics. Taking the side of software customers and independent software developers, I've been attending meetings of the Drafting Committee and NCCUSL, to identify and point out strengths and weaknesses in UCITA (then Article 2B) since the second Article 2B Drafting Committee meeting, in early 1996.

The Drafting Committee's responses to criticism has been disappointing. Proponents of UCITA dismiss criticisms, speaking of them as "fabricated or uninformed claims of opposition." Even in the drafts of UCITA itself, we see: "[M]any public statements have been made about the effect of Article 2B on consumer protection. Most are political efforts to mislead."

As a proposed revision to the Uniform Commercial Code, Article 2B, was co-developed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) and the American Law Institute (ALI). At its May 1998 annual meeting, the ALI membership approved a motion stating that Article 2B "should be returned to the Drafting Committee for fundamental revision." The revisions were not made, and the ALI withdrew from the Article 2B process in 1999. The ALI co-authors all revisions to the UCC. Without its support, NCCUSL renamed Article 2B as the Uniform Computer Information Transactions Act, UCITA.

This article looks at some of the key criticisms of UCITA. There are many other significant problems with UCITA. These are just examples, chosen to get across the point that there are big problems with this bill, in a short article.

Opposition to UCITA

The first thing to realize about the Uniform Computer Information Transactions Act (UCITA) is that it lacks the support of the software industry.

Oh, sure. Software publishers like UCITA. And software publishers are important players in the software industry. But if West Publishing supports a bill, does that mean that the bill has the support of the legal industry?

The Association for Computing Machinery opposes UCITA. So does the Institute for Electrical and Electronic Engineers. These are the two main professional societies in the field. Software Engineering, by the way, is a licensed profession in Texas, Ontario, and British Columbia. The American Society for Quality opposes UCITA, at the encouragement of its Software Division. The Independent Computer Consultants Association, which represents individual software developers and small software service providers, sent a representative to several UCITA / Article 2B drafting committee meetings, proposed changes (which weren't adopted) and eventually came out in opposition to UCITA. The Free Software Foundation, which supports the development of open source software products like Linux, opposes UCITA. The Software Engineering Institute, which was formed by the U.S. Department of Defense to further the state of software practice, and which is highly influential in the field, opposes UCITA. These are substantial organizations. They are not wild-

eyed consumer advocates. They are major players in the software industry. They all, along with several other developers' groups, oppose UCITA.

Proponents of UCITA have suggested that the primary opposition to UCITA comes from consumers. Certainly, consumer advocates oppose UCITA. As do the Attorneys General of Arizona, Arkansas, California, Connecticut, Florida, Idaho, Indiana, Iowa, Kansas, Maryland, Minnesota, Mississippi, Missouri, Nevada, New Jersey, New Mexico, North Dakota, Oklahoma, Pennsylvania, Tennessee, Vermont, Washington, West Virginia, Wisconsin and the Administrator of the Georgia Fair Business Practices Act. The staff of the Federal Trade Commission have written two reports that are highly critical of UCITA.

But the opposition to UCITA is much broader than this. Many intellectual property specialists oppose UCITA, including 50 intellectual property law professors, the American Intellectual Property Law Association, and the Committee on Copyright and Literary Property, the Communications and Media Law Committee and the Entertainment Law Committee of the Association of the Bar of the City of New York. The press oppose UCITA. The libraries oppose UCITA. The entertainment industry opposes UCITA. And so do large commercial software customers.

Unreasonable, Surprising Terms

During the UCITA drafting process, lawyers representing large corporate customers said repeatedly that UCITA would force them to change their business practices. Their concern is that software contracts contain remarkably aggressive terms. They don't think that they would be bound by the worst of these terms in mass-market contracts under current law, but these terms certainly seem enforceable under UCITA, no matter who pays for them or who installs them on their company's computer system. Therefore, these corporate counsel said, they think that they will have to get involved in a review of every software acquisition and installation made by their companies.

Here is an example of the problem. Go to Intel's website, at www.intel.com/home/funstuff/webapplets/album2/album2.htm. If the page is the same as it was on December 19, 1999, this page advertises the Intel Photo Album II applet. It says,

"Use the Photo Album II applet to add high-tech image transitions to your Web pages. Origami, Unseen Wind and Brush are just a few of the effects that will surprise and delight your viewers."

The product category appeals to consumers, to relatively junior designers of websites, and to other people who would not normally have much power to bind a corporation to significant contracts. This product is free. No one has to sign a cheque or a purchase order to get it. It can be obtained and used at a company with no review by anyone involved with the management of that company.

Intel's page provides two sets of samples of use of the product:

- the Lincoln High School Student Activity Center and
- TransWorld Travel

Neither organization (Lincoln High School or TransWorld Travel) would be classed as a consumer under UCITA.

Buried in the license agreement (at www.intel.com/cpc/webapplets/album2/agreement.htm), starting 577 words into a 1228 word document, is the following text:

"Licensee agrees that all works of authorship, inventions, improvements, developments making use of the Applet or any portion of the Applet, solely or in collaboration with others, as well as all patents, copyrights, trade secrets, trademarks and other intellectual property rights therein and thereto (collectively, "Developments"), are the sole property of Intel. Licensee agrees to assign (or cause to be assigned) and does hereby assign fully to Intel all such Developments."

The next section puts licensees under a duty of disclosure to Intel.

Suppose that you are the corporate counsel in a company that has a public web site and an internal site that includes a password-protected section that presents new technical ideas and specifications for your advanced product's group review. The ideas presented are valuable trade secrets.

Unfortunately, one of your company's technical staff downloaded the Intel Photo Album II applet, didn't read or understand all of the legal terms, and used it on the public web site and to create the New Ideas presentation. If Intel's license clause is enforceable, Intel now owns part of your public site, and your secret presentation.

In early versions of Article 2B, a clause like this might have been knocked out. In Section 2B-308 (12/12/96 draft), Article 2B, said:

"A term does not become part of the contract if the term creates an obligation or imposes a limitation which: (1) the party proposing the form should know would cause an ordinary and reasonable person acquiring this type of information and receiving the form to refuse the license if that party knew that the license contained the particular term."

Unfortunately, even this weak exclusion of surprising, material terms is not part of UCITA. Had you reviewed the license, you would probably have rejected this term immediately and told the staff member not to use Photo Album II for any purpose inside your company. But you didn't review the terms, and. So if they used the product, how can you protect your company's work products and secrets from Intel?

You might try arguing that the term is unconscionable under UCITA Section 111, but courts are rarely receptive to a business' plea for relief from a contract term on grounds of unconscionability. You might try arguing that this term should not be enforced because something about it violates a fundamental public policy, but I'm not sure which one you would cite.

Clearly, before allowing your company to use any piece of software, clip art, downloaded information, or anything else that can be construed as computer information, you must review each and every associated license, even for products that cost nothing or only a few dollars. Otherwise, the intellectual property of your company is at risk.

E-Mail Receipt Rules

UCITA 102(a) (53) defines "receive" as taking receipt and 102(a)(52) (II) defines "Receipt" to mean "in the case of an electronic notice, coming into existence in an information processing system or at an address in that system in a form capable of being processed by or perceived from a system of that type by a recipient, if the recipient uses, or otherwise has designated or holds out, that place or system for receipt of notices of the kind to be given and the sender does not know that the notice cannot be accessed from that place." Under Section 215(a) "Receipt of an electronic message is effective when received even if no individual is aware of its receipt."

This definition creates serious problems.

- It leaves you defenseless in situations in which you never had access to a message that was sent to you, because you "received" that message, but you never got it or could never read it.
- It creates serious risks for anyone who uses filters to automatically purge pornography, get-rich-quick schemes, and other trash from their electronic mail.
- It creates significant costs and risks for corporations who receive electronic mail.

Defenseless Against Non-Receipt

Suppose that your e-mail address is yourname@YourISP.com. And suppose that you engaged in an electronic transaction (such as downloading software from a web site) and that the associated non-negotiable, visible-only-after-the-sale license specified in the fine print that all legal notices could be sent to you by e-mail to yourname@YourISP.com. By clicking OK to that license, you have designated your internet service provider

(in this case, YourISP) as the place or system for receipt of such notices. When the other party sends a message, UCITA says that the message has been received by you when it reaches yourisp.com in good shape.

The fact that the message reached YourISP.com does not mean that it will reach you. There can be a problem at YourISP's server (they lose your messages) or a transmission problem (the message gets corrupted or lost en route to your machine) or the message might be corrupted at your computer (maybe by a virus or by a bug in your mail program). In any of these cases, you don't see the message, but UCITA says that you have received it.

Note the difference between this situation and the mailbox rule. Under the mailbox rule, we create a presumption that a letter has been received with a certain time after it is sent. But that presumption is refutable. In this case, even though the message has never reached any screen that lines up with your eyeball, UCITA says that as a matter of law, you have seen it.

You Can't Filter Your E-Mail

The second issue is the filtering issue. According to a recent article in the Boston Globe, a huge proportion of circulating e-mail is spam, unsolicited junk mail. For example, 15-30% of the e-mail received by America Online is spam. The article quotes estimates that pornographers are the source of 30.2 percent of the spam on the Internet, followed by get-rich-quick and work-at-home schemes (29.6 percent of spam). People who receive a lot of electronic mail often use filters, programs that detect spam and erase it before they ever have a chance to notice it.

Suppose that you use a filter that wipes out any message that originates from the domain, SpamSender.com. Someday, someone might send you a legal notice via SpamSender.com. If your filter wipes out messages from that source, you will never see the legal notice. But under UCITA, that notice will have full legal effect because it reached your system, even though it stood no chance of reaching your eyeball.

Under UCITA, anyone who engages in electronic commerce (such as electronic banking) will probably end up with e-mail notification clauses in their contracts. If they filter the junk out of their electronic mail, they risk being held accountable for having received messages that their computer completely hid from them (as it was supposed to do). A risk-averse person will not and should not use spam filters because of the risks of filtering that are imposed on them by UCITA. Under UCITA, these people will have to hand filter every offensive piece of pornography that is dumped to their system.

Corporate E-Mail

UCITA's mailbox rule creates challenges for the corporation as well. Corporations receive a lot of spam. Today, in many companies, much of this spam is filtered (identified and deleted) as it comes into the system. The corporate computers identify the spam as having a traditional title or as originating from an internet service provider that routinely hosts spammers. As they filter, some legitimate mail is inevitably lost. So, imagine yourself as corporate counsel. Do you tell your company they can continue to automatically filter mail? Or, because of the UCITA-imposed risks on filtering, do you say that they have to stop filtering and actually inspect / read every message? How much of your company's time are you willing to waste on this? How much of their time are they willing to let you waste?

Another problem is the difficulty of finding skilled network and system administrators in the current job market. Under UCITA, mail sent to employee@Corporation.com has been received when it reaches Corporation's server, but if Corporation is having trouble breaking in a new system administrator, a lot of mail might never reach any of Corporation's employees. Lost e-mail is not like lost letters that go to the wrong person but can be rerouted back. Losing a day of e-mail is like sending all of your company's mail to the shredder. It's gone. And if you just lose a percentage of it, you might not even realize that you have a lost mail problem until your company is held accountable for notices that no one ever actually had the opportunity to read.

Known Defects

One of the fundamental assumptions of UCITA is that "The complexity of software products makes them inherently imperfect." "Minor flaws ("bugs") are common in virtually all software." "In fact, the idea of perfect software is a goal or aspiration not presently attainable, at least not without exorbitant costs that would drive many thousands of small companies out of the business."

This is a straw man. In the Article 2B/UCITA meetings, the debate about accountability for defective software was not about whether software should be perfect. As an expert on software quality control, I wrote a memo for the UCITA / 2B drafting committee explaining in detail that it is impossible to exhaustively test software products or to prove by testing that a product is defect free.

But what about known defects? It might be impossible to find all the defects, but that issue doesn't apply to the defects that were actually found. In mass-market software, a large proportion of defects (often the vast majority of them) that reach customers are discovered and intentionally left unfixed by the publisher before the product is released. Several representatives of the software engineering community, and Ralph Nader's representative (Todd Paglia) and I repeatedly proposed that software companies should be held accountable for defects that they knew about at the time of sale and chose not to disclose. These proposals typically barred consequential damages for defects that were unknown or that were revealed to the customer in the product documentation (which makes it possible for customers to avoid or mitigate losses caused by known defects). Additionally, we suggested that damages for known defects in mass-market products could be limited to demonstrable out-of-pocket expenses and capped, perhaps at $500 per customer. These proposals were rejected.

One of the arguments made by UCITA proponents was that failure to disclose a known defect should be dealt with under the law of fraud. Sometimes, such a failure might be fraudulent—as when the seller knowingly makes a false statement about the product. But to the best of my knowledge, in the sale of goods, mere failure to mention a known defect, even a material defect, does not give rise to fraud liability. We didn't ask for fraud liability. We asked that software publishers be held accountable for *breach of contract* if they knowingly delivered a defective product without revealing the defect.

Our proposal grew out of the special recognition in UCITA that software companies need a break because of the alleged inevitability of defects. Some of the details of that break include the de facto elimination of the requirement that warranty disclaimers and damage limitations be conspicuous and made available to the customer before the sale, elimination of the principle of minimum adequate damages, the adoption of a rule that excludes incidentals and consequentials for defects even when the agreed remedy fails, and the adoption of a more seller-favorable definition of material breach. Our proposal was a tradeoff—let the new law reduce publisher risk for losses caused by previously undiscovered defects or defects that were disclosed to the customer, but reduce the customer's risk of losses caused by defects that were known and left hidden.

I believe that within the current state of software engineering, it is usually commercially unreasonable to attempt to create a defect-free software. Based on that belief, I have no objection to limiting the liability risk of publishers and other software developers for defects that they didn't know about or that they were honest enough to disclose, even if those defects cause substantial losses. But what if the state of the art improves?

Watts Humphrey raised this issue at several meetings of the UCITA / 2B drafting committee. Professor Humphrey is a former vice-president of IBM, author of seven books on software engineering, and widely respected in the field. He presented data to the drafting committee that showed that new development methods were succeeding in producing very large, very complex products that were nearly defect free. Humphrey's comments at the drafting committee meetings were largely ignored. Ultimately, his points were reiterated by the Director of the Software Engineering Institute, Stephen Cross, who wrote,

"The Article 2B draft assumes that software products are inherently defective and that the current quality practices in the industry will not improve. The history in other fields demonstrates that as a technology matures,

the marketplace becomes more sensitive to quality issues. In fact, software quality is a growing concern to the user community, and software quality is an active current area of study. Considerable progress is being made. . . . The Article 2B proposal makes no technical sense. We feel that it would inhibit natural market forces, damage users, and ultimately limit the health and growth of this industry. While we appreciate the efforts that have been made to produce the UCC-2B draft, we must urge you to oppose its adoption."

Obvious Defects and Material Breach

Under current law, contracts for packaged software (products that are delivered to the customer without extensive customization) are governed by Article 2 of the Uniform Commercial Code. Article 2 allows the customer to reject a product for any failure to conform to the contract that is detected during a relatively brief inspection period. This is the perfect tender rule.

UCITA retains the perfect tender rule for mass-market software but eliminates it for most business software transactions. To reject the product under UCITA, the business must prove a material breach of contract. (Even then, under Section 803, the contract can specify that the customer simply has no right to cancel.) The elimination of perfect tender undermines the credibility of a customer's threat to cancel the contract unless obvious defects are fixed. It reduces the bargaining power of the customer.

After the initial inspection period has passed, the mass-market customer can cancel the contract only if the breach is material. For most defects, the consumer or business customer will have to show a material breach in order to prove entitlement to a refund.

UCITA creates a new, more seller-friendly definition of "material breach." Here is the definition under UCITA:

UCITA 701 (b) A breach of contract is material if:

(1) the contract so provides;

(2) the breach is a substantial failure to perform a term that is an essential element of the agreement; or

(3) the circumstances, including the language of the agreement, the reasonable expectations of the parties, the standards and practices of the business, trade, or industry, and the character of the breach, indicate that:

(A) the breach caused or is likely to cause substantial harm to the aggrieved party; or

(B) the breach substantially deprived or is likely substantially to deprive the aggrieved party of a significant benefit it reasonably expected under the contract.

In contrast, here is the definition of a material breach from the Restatement of Contracts Second, Section 241:

In determining whether a failure to render or to offer performance is material, the following circumstances are significant:

(a) the extent to which the injured party will be deprived of the benefit which he reasonably expected;

(b) the extent to which the injured party can be adequately compensated for the part of that benefit of which he will be deprived;

(c) the extent to which the party failing to perform or to offer to perform will suffer forfeiture;

(d) the likelihood that the party failing to perform or to offer to perform will cure his failure, taking account of all the circumstances including any reasonable assurances;

(e) the extent to which the behavior of the party failing to perform or to offer to perform comports with standards of good faith and fair dealing.

A Hypothetical on Material Breach

To see the difference between the two material breach standards, imagine that you are an attorney representing a customer of a packaged software product with a non-negotiable click-through license. (This might but need not be a mass-market product.) Suppose further that the software had a defect that your client considers serious. The vendor does not yet have a fix for this defect and has made no promise as to when (if) it will be fixed. Your client wants a refund for the software. The vendor (who published the software) has refused to give the refund. You have discovered that the defect was known to the vendor at the time of sale. It was not documented or revealed to the customer.

Under UCITA and under the Restatement, your customer is entitled to a refund if she can prove a material breach of contract.

Under UCITA, Section 701(b)(1), the breach is material if the contract says it is. The contract was written by the vendor, and so for the vendor, the UCITA standard for material breach *by the customer* is whatever the vendor's contract says it is. However, there's probably nothing in the vendor-written contract that will be useful for the customer.

Under Section 701(b)(2), the breach is material if it is a substantial failure to perform a term that is an essential element of the vendor-drafted agreement. It's unlikely that the vendor would write a contract that contains, as an essential term, a requirement that the product do something that it cannot do. This won't help your client either.

That leaves UCITA's Section 701(b)(3), which allows your client to recover for substantial harm or for being substantially deprived of a significant benefit. How much harm is enough to be called "substantial"? How significant does the benefit have to be before it is "significant" and how badly must the program misbehave before that benefit is "substantially" gone? These are questions of fact that will often leave the vendor with room to argue that a problem is not significant or substantial enough.

The Restatement analysis will be much more favorable to your client. Under the Restatement, your client's case will be evaluated under five factors:

(a) the extent to which your client is deprived of the benefit. This is like the UCITA standard except that if the other factors are favorable to the client, a breach can be material with a less substantial deprivation of a less significant benefit.

(b) the extent to which your client can be adequately compensated. If the vendor won't pay incidental or consequential damages and won't quickly fix the defect, a customer might reasonably and legitimately expect a refund (so that she can go buy something that works) rather than a partial refund.

(c) the extent to which the party failing to perform will suffer forfeiture. A vendor who sells many copies does not suffer a forfeiture when one customer cancels the contract for one copy.

(d) the likelihood of cure. The vendor isn't making any promises.

(e) The extent to which the behavior of the party failing comports with standards of good faith and fair dealing. You can reasonably argue that the vendor's delivery of known, undisclosed defects fails to reflect good faith and fair dealing.

Lack of compensation, lack of cure, no risk of forfeiture, and sharp practices by the seller are a common combination in the industry. It speaks strongly to the bias of UCITA that these are taken out of the equation.

Restrictions on Speech

UCITA Reporter Ray Nimmer complained of "distortions" in the debate on UCITA, identifying as a "misrepresentation" "that UCITA allows licensors to prevent licensees from commenting about the products. This allegation makes nice copy and superficial impact, but is simply untrue. You can scroll through the UCITA draft and will not find any such provision."

Opponents quickly point to UCITA section 102(a) (20), which defines “contractual use restriction” as “an enforceable restriction created by contract which concerns the use or disclosure of, or access to licensed information or informational rights, including a limitation on scope or manner of use.” Section 307(b) states that “If a license expressly limits use of the information or informational rights, use in any other manner is a breach of contract.” Under the statute’s own definition, a nondisclosure clause is a contractual use restriction. Under Section 307(b), such a restriction is enforceable.

These provisions may keep vital information from the marketplace. Consider the following restrictions, downloaded (July 20, 1999) from www.mcafee.com, the website for VirusScan, a mass-market software product, on July 20, 1999.

"The customer shall not disclose the results of any benchmark test to any third party without McAfee's prior written approval."

"The customers will not publish reviews of the product without prior consent from McAfee."

Clauses like these are enforceable in traditional, negotiated licenses, and they are used to block magazine reviews. UCITA arguably extends the enforceability of such clauses even in mass market products. Perhaps they will eventually be found to conflict with public policy but until then, the plain language of UCITA will have a chilling effect on criticism of mass-market products.

Security Problems Caused by Self-Help

UCITA section 816 allows software vendors to place disabling codes in software and to activate them remotely (such as by sending an e-mail) to shut down a customer’s use of the product.

Such disabling codes create a hole in the customer’s system security. When a licensor leaves a back door in its code, something that allows them to shut the software down with a single message:

- Sometimes, a defects in the vendor's software will produce a shutdown by accident. (UCITA regards software defects as inevitable, so surely we can expect some defects in the parts of the software that govern self-help.)
- Sometimes, a third party will discover how to shut systems down this way. (For example, the third party might by a former employee of the software publisher.) Such a person might shut systems down for the fun of it or he might engage in extortion, either of the vendor or the customer. *You might say, yes, there are criminals who do these things, but they are beyond our control. But in this case, the criminal is exploiting a security hole that is authorized by Section 816. If self-help were banned, this risk would not exist.*

UCITA section 816 remedies for wrongful use of such codes are probably not triggered if the software is shut down accidentally or by a third party (such as a cracker who learns the code or a disgruntled former employee of the vendor).

Self-help was portrayed in the UCITA meetings as something essential to protect the interests of small licensors. However, the only group attending the UCITA meetings that represents only small licensors, the Independent Computer Consultants Association, urged NCCUSL to ban self-help. Instead, ICCA recommended that a party wishing to terminate use of its software should be allowed to proceed by injunction and recover attorney's fees. The availability of attorney's fees goes a long way toward making it possible for a small licensor to be able to afford to obtain the injunction. This proposal was rejected by the drafting committee.

Transfer Restrictions

Under UCITA, almost all software-related transactions will be licensing transactions. When a consumer buys a copy of Microsoft Word and a copy of a book about the program, the software transaction would be a license while the book transaction is a sale, even if the two items were side by side, the customer bought them both from the same cashier, and the software license was not available to the customer until after

she paid for the product and took it away. Under UCITA 102(a)(42) a transaction can be a license even if the licensee is given title to the transferred copy.

This is a shift from long-established treatment of intellectual property in the mass market. To see the history of this issue in copyright law, shepardize *Jewelers' Mercantile Agency v. Jewelers' Pub. Co.*, 155 N.Y. 241 (1898) (rejected the fiction of a lease offered to all comers that restricted transfer of the book and use of information in it); *Bobbs-Merrill Co. v. Straus*, 210 U.S. 339 (1908) (rejected a restrictive notice on a book that prohibited the buyer from reselling the book for less than a minimum price. Under the first sale doctrine, publisher lost its property interest in an individual copy of a book once it sold that copy. The restrictive notice could not transform a sale into a license); *RCA Mfg. Co. v. Whiteman*, 114 F.2d 86 (2d Cir. 1940) (Licensing language on record albums could not convert a mass-market sale into a license.) For patent law, look at the doctrine of exhaustion, starting with *Motion Picture Patents Co. v. Universal Film Manufacturing* Co. 243 U.S. 502 (1917).

According to an article by the Connie Ring, Chairman of the UCITA drafting committee. "UCITA is intended neither to avoid nor to contradict the large body of existing federal intellectual property law." Others vigorously disagree. For example, the American Intellectual Property Law Association protested to NCCUSL that UCITA "eliminates the 'first sale' doctrine" (which allows the owner of a copy to sell it or give it away). Under UCITA 503(2),

"a term prohibiting transfer of a party's interest is enforceable, and a transfer made in violation of that term is a breach of contract and is ineffective."

A vendor who puts a no-transfer clause in the license achieves a market-wide restriction--equivalent to elimination of the first sale doctrine. By allowing vendors to enforce such restrictions in the mass-market, UCITA allows them to evade the federal balancing of private and public rights in intellectual property.

UCITA 503(2) has several consequences. For example in the face of such a restriction:

A A consumer who buys a computer game cannot lawfully give the game to his sister after he gets tired of playing with it. (Don't confuse this with giving the sister a copy, which is already banned under the Copyright Act. 503(2) says that the consumer cannot erase any local copy on his machine, put the original disk back in the original box, and then give that disk and box to the sister.)

A A consumer who buys a copy of an encyclopedia on CD cannot donate the used CD to her local library.

A Used bookstores and used record stores will no longer be able to sell used software. The marketplace in used software is eliminated by UCITA.

A A business that sells substantially all of its assets to a second business cannot transfer its software to the second business, not even the mass-market software that came pre-loaded on the computers bought by the business. The selling company will have to either wipe the hard disks or inventory each computer, finding every program, every piece of clip art, clip music, and downloaded data, and get permission of the original licensor to transfer the item to the buying company. The transaction costs of this (the cost of inventorying, finding all the licensors, getting all the permissions) will be enormous.

Consumer Warranty Protection

Among the most important ways that UCITA affects consumers are its revisions to warranty law. I think that the three most important effects are these:

A UCITA eliminates the longstanding requirement that warranty disclaimers be conspicuous and available to the customer at or before time of purchase.

A UCITA pulls consumer software transactions out of the scope of the Magnuson-Moss Warranty Improvement Act and of other consumer protection statutes whose scope is specified as sales of goods.

A UCITA pulls the teeth out of the express warranty by demonstration, making it much harder to hold publishers' accountable for their staffs' product demonstrations at trade shows, retailers, and so on.

Warranty Disclaimers

Under Article 2-314 of the Uniform Commercial Code, a seller can exclude the implied warranty of merchantability by conspicuously disclaiming it. The exclusion clause in a shrink-wrapped software contract might be conspicuous on its page if it is set apart from the rest of the text by being in all capital letters. But such a disclaimer cannot be considered conspicuous at time of sale (except for people with X-ray vision) because it is inside the box and not available for viewing by the customer.

Over the past century, courts have consistently refused to enforce post-sale disclaimers of the implied warranty of merchantability. Under UCITA, such disclaimers are fully enforceable in a click-through or shrink-wrapped license even if they are completely unavailable to the customer before or at the time of the sale.

Magnuson-Moss Act

The Magnuson-Moss Warranty Act provides consumers with additional warranty rights, beyond the Uniform Commercial Code. For example, under the Act, a seller who provides *any* written warranty with a consumer product or who sells you a service contract (such as extended technical support) for the product may not disclaim implied warranties.

The Magnuson-Moss Act applies to all consumer goods. Consumer goods are those which are "normally used for personal, family, or household purposes." This is a broad definition, and under current law, it almost certainly includes personal computers and most of the types of software that you'd buy in software stores.

According to the Federal Trade Commission

"The Act applies to written warranties on tangible personal property which is normally used for personal, family, or household purposes. This definition includes property which is intended to be attached to or installed in any real property without regard to whether it is so attached or installed. This means that a product is a `consumer product' if the use of that type of product is not uncommon. The percentage of sales or the use to which a product is put by any individual buyer is not determinative. For example, products such as automobiles and typewriters which are used for both personal and commercial purposes come within the definition of consumer product. Where it is unclear whether a particular product is covered under the definition of consumer product, any ambiguity will be resolved in favor of coverage.

The Software Publishers Association's *Guide to Contracts* considered the applicability of the Magnuson-Moss Act and concluded that "It is reasonable to assume that software purchased for home computer use would be covered by the Act."

There are no published court rulings that have settled the question of the applicability of the Magnuson-Moss Act to software, but it is generally believed that courts would rule that the Act applies to consumer software. Two related lawsuits, *Stuessey v. Microsoft* and *Microsoft v. Manning* included a claim for violation of the Magnuson-Moss Act. In these cases, because of compression-related problems "about three in 1,000 [people] lost data after using MS-DOS 6.0" (*Manning*, p. 606). In these two suits, customers sued for consequential damages (*Stuessey*) or for a free upgrade to DOS 6.2 (*Manning*). Microsoft had disclaimed the implied warranty of merchantability but the Magnuson-Moss Act voids the disclaimer and reinstates the implied warranties. Apparently, the court accepted the applicability of the Magnuson-Moss claim because, despite Microsoft's disclaimer, the *Manning* court applied the disclaimed warranty, saying that "the software was not fit for the ordinary purpose for which software is used."

UCITA pulls software out of the scope of sales-of-goods law by defining the transaction as a license. Under UCITA, you are buying an intangible, a license, not goods. This pulls software outside of the scope of the Magnuson Moss Act and of analogous state laws, while allowing proponents of UCITA to claim that UCITA does not change consumer protection laws. (It doesn't, in this case. It merely takes software outside of their scope.) For the first two years that I pointed this out, proponents told me that I was misrepresenting the effect of UCITA (Article 2B). These days, they say instead that the Magnuson-Moss Act was never intended to apply to software.

Warranty By Demonstration

Software products are complex. Customers often buy them in reliance on demonstrations made by salespeople at stores and trade shows.

The Uniform Commercial Code recognizes that customers rely and demonstrations. Under Article 2-313(1) (c) " Any sample or model which is made part of the basis of the bargain creates an express warranty that the whole of the goods shall conform to the sample or model."

UCITA gives vendors two ways to give demonstrations that would create warranties under Article 2 but that do not create warranties under UCITA.

- First, Under Section 402(a)(3)

" Any sample, model, or demonstration of a *final* product which is made part of the basis of the bargain creates an express warranty that the performance of the information will *reasonably* conform to the performance of the sample, model, or demonstration, *taking into account differences* that would appear to a reasonable person in the position of the licensee between the sample, model, or demonstration and the information as it will be used." (Italics mine.)

> If the vendor uses a preliminary "demo" version instead of a final version, then no warranty is created even if the customer thinks she is looking at the final version. Note that this is not fraud if the vendor does not intend to mislead the customer. Also, UCITA substitutes the simple requirement of conformance with "reasonable" conformance. A bright line test becomes an issue of fact for the jury. Under current law, a customer can know with certainty that there was a warranty and it was breached, but under UCITA, the customer cannot. UCITA provides an additional defense for the vendor to take to the jury, the " differences" that should be noticed by a "reasonable" customer.

- Second, under Section 402(b)

"[A]n express warranty is not created by: (2) a display or description of a portion of the information to illustrate the aesthetics, appeal, suitability to taste, or the like of informational content;

> People buy products on the basis of their user interface. If a vendor demonstrates a product or publishes pictures of the product's screens, but delivers a different version that is less appealing, less visually pleasing, harder to use, etc., the customer has no claim for breach of warranty. Such a situation might or might not be fraudulent, depending on whether the publisher intended to mislead people. Independently of the fraud question, under Article 2 this would be a breach of contract. Under UCITA, it is not.

In Closing

This article reviewed a few of the problems with UCITA. There are many others.

The UCITA drafting process reflected a cozy relationship between the software publishing industry and the drafters. The drafting committee meetings were dominated by lawyers representing information publishers. During the drafting process, the Reporter wrote a book with a lobbyist for the Software Publishers Association and he accepted at least one consulting contract (on an allegedly unrelated matter) with Microsoft.

The UCITA bill is a sweetheart deal for software publishing corporations, for database access providers (West and Lexis played significant roles in UCITA and will benefit from their increased ability to restrict your right to use court cases that you download from them), for computer manufacturers (who can bring their machines under UCITA), and maybe for some other goods vendors (UCITA-like provisions are being pushed at the UCC Article 2 revision committee.)

The level of bias of UCITA is not appropriate to a commercial statute.

Appendix G
Braucher-Linzer Motion
[The ALI adoption of this motion and the failure of the drafting committee to comply caused ALI to drop out of the UCC Article 2B drafting process and the project's renaming by NCCUSL as UCITA.]

To: Members of the American Law Institute

From: Jean Braucher and Peter Linzer

Re: Assent issues in Proposed UCC Article 2B

Date: May 5, 1998

We believe that the Tentative Draft (April 15, 1998), Uniform Commercial Code Article 2B, takes a flawed approach to basic issues of contract law, particularly concerning assent. This is more than a philosophical or jurisprudential difference of opinion; this new UCC Article would affect billions of dollars in transactions involving software and information. While problems with many sections of the draft are detailed in the accompanying examples and discussion, we do not ask the membership to adopt specific drafting solutions during our Annual Meeting. Rather, we think it appropriate for the Institute membership to express its disapproval of the underlying philosophy exhibited in the current draft and to ask the Drafting Committee to produce legislation in keeping with principles of freedom of contract expressed in the Restatement (Second) of Contracts.

Moved: The American Law Institute membership supports the following statement:

> The current draft of proposed UCC Article 2B has not reached an acceptable balance in its provisions concerning assent to standard form records and should be returned to the Drafting Committee for fundamental revision of the several related sections governing assent.

MEMORANDUM IN SUPPORT

The Draft reflects a persistent bias in favor of those who draft standard forms, most commonly licensors. It would validate practices that involve post-purchase presentation of terms in both business and consumer transactions (using "shrinkwrap" and "clickwrap"), undermining the development of competition in contingent terms, such as warranties and remedies. It also would allow imposition of terms outside the range of reasonable expectations and permit routine contractual restrictions on uses of information traditionally protected by federal intellectual property law. A fundamental change in approach is needed. The purpose of this broad Motion is to reject the Draft's general approach to finding contractual assent, an approach found in several interrelated sections (Sections 2B-203, 2B-207, 2B-208, 2B-111 and 2B-304). While these Sections as written should be stricken, simply striking them will not produce an acceptable draft without some rethinking and redrafting. The purpose of this Motion is to return the Draft to the Drafting Committee for that work. After giving some examples of how the Draft in its present form would work, we discuss more generally the provisions that produce these results.

Examples

Two cases illustrate many of the problems with proposed Article 2B's treatment of assent to standard forms and show how the Draft deviates from long-standing contract law:

> Case 1: User Co. sends (whether by mail, fax or e-mail) an order form for accounting software to Producer Co., which responds with an acknowledgment. The two forms conflict on material terms. User Co.'s form provides for delivery of merchantable software and for resolution of disputes by litigation in its home state. Producer Co.'s form disclaims the implied warranty of merchantability and provides for dispute resolution by arbitration. It also provides that Producer Co. may change the terms of the contract in the future by giving notice to User Co. Producer Co. then ships disks containing the software to User Co., and User Co. pays. (Alternatively, Producer Co. might deliver the software on line.) During installation of the software, a technician at User Co. clicks through a screen that states that licensee assents to a standard form license. It is necessary to click on this screen to access the software. The license contains the same terms as those in Producer Co.'s acknowledgment.

Many courts would now apply Article 2 to this transaction and find that the terms of the transaction are those on which the two forms agree, plus the gap-fillers of Article 2. Section 2-207(3). This would mean that User Co. would get an implied warranty of merchantability, disputes would be subject to resolution by litigation, and the "future changes" clause would not become part of the contract. Under Article 2B, the terms would be those of the "click through" license, and Producer Co. would get its warranty disclaimer and its arbitration term. Sections 2B-203(b)(1)(A) and (c)(2), 2B-207, and 2B-111. In addition, Producer Co. would have the right under Article 2B to change even material terms of the contract, by giving notice, and User Co. would not have the right to cancel if it did not like the changes. Section 2B-304. Article 2 has no comparable provision to give blanket validity to "future changes" without further assent of the other party. Compare current Article 2, Section 2-209(1)(permitting modification, which requires both parties to agree).

> Case 2: User, an individual, wants personal financial management software for household use. User is interested in finding a provider who includes in the deal a period of free telephone help. User goes to Software Retailer and looks at the boxes for this type of software. None of them have terms on the outside of the box. User asks an employee what the terms inside the boxes say, but employee says she does not know, and she refuses to let User open the boxes. User goes home and logs on to the Internet and attempts to find license terms that include a period of free telephone help. Unfortunately, User discovers that many producers do not put their licenses or warranties on their Web sites. User orders some software on line and pays by giving a credit card number. Producer Co. sends a disk to User. In order to access the software, User is asked during installation to assent to a license by clicking on a screen. User clicks on the screen. The software license terms include a warranty stating that the disk is free from defects in material and workmanship and giving a remedy of replacement of the disk. The license also states that the software itself, as opposed to the disk, is provided "AS IS," that User may not publish a review of the product without Producer Co.'s prior written permission and that telephone help is provided at $3 per minute. User discovers a bug in the program and calls Producer Co. for telephone help. Producer Co. charges $3 per minute, even though User is calling to report the bug and get help on how to deal with it. User decides to write a negative review of the product for a computer magazine, but Producer Co. refuses to give permission for its publication and threatens to sue for damages.

Again, many courts now would apply Article 2 to the transaction, and they would not enforce the license delivered after purchase, making the warranty disclaimer and "no review" term ineffective. In addition, the

Magnuson-Moss Warranty Act probably applies to the transaction, so that warranty terms must be made available prior to purchase on request. 15 U.S.C. Section 2302(a); 16 C.F.R. Section 702.3(a)(2). Thus, Retail Store violated Magnuson-Moss by not providing access to the content of written warranties when asked about them by User. Also, implied warranties cannot be disclaimed when a written warranty is given, so that Producer Co. has also violated Magnuson-Moss. 15 U.S.C. section 2308.

Under Article 2B, however, User would be bound to all terms in the "click through" license, unless they are unconscionable. Sections 2B-208(a), 2B-111. The right of refund in Section 2B-208(b) would be lost when User clicked. The implied warranty could be effectively disclaimed in terms provided after purchase, unless Magnuson-Moss pre-empts Article 2B on this point (which may well be the case, although licensors are not warned of that possibility in Article 2B). Also, under Article 2B, there is an attempt to disown Section 211(3) of the Restatement (Second) of Contracts, which makes bizarre or oppressive terms unenforceable, whether in commercial or consumer contracts. See Section 211, comment e. Compare Sections 2B-207 and 2B-208 and Reporter's Notes to those section. (See especially Reporter's Note 1 to 2B-208.) Thus, User would not have the "reasonable expectations" doctrine as a tool to challenge the enforceability of the "no reviews" term. Because Article 2B validates post-transaction presentation of terms, the fact that the term was in a "click through" license may not be enough to show "procedural" unconscionability, making it hard to use that theory because unconscionability case law usually requires both substantive and procedural unconscionability.

Discussion

Standard form contracts are a fact of commercial life, with significant economies of scale in the production of contracts, akin to those achieved in the mass production of goods and services. This point is made in the Restatement (Second) of Contracts, Section 211, comment a. On the other hand, the Restatement also recognizes significant costs associated with standard form contracts, including the problem that those drafting them "may be tempted to overdraw." Id. at comment c. The very ease of drafting forms has led to their proliferation, making it impossible for either individuals or businesses to read and understand all the contracts to which they purportedly "assent." The idea that reading form documents is not realistic is embodied in sales law, existing Article 2, Section 2-207, which finds assent and provides gap-filling terms even though forms exchanged are not mirror images, in recognition that commercial sellers and buyers do not read and reconcile the forms they exchange.

Despite these widely accepted realities, Article 2B adopts a hard version of fictional assent to form contracts. While the Reporter's Notes claim that the approach serves freedom of contract, it would in fact undermine freedom of contract in favor of regulation by the one who drafts the form. In addition to dictating limited quality assurance and remedies, the drafter could impose form terms restricting uses of information traditionally protected by federal intellectual property law. The Reporter's Notes also portray Article 2B as a collection of "default rules" that can be displaced by the parties' agreement. But in the vast majority of transactions, including acquisitions by business users, the "parties' agreement" will be the terms of the drafter's form, first presented to the user after order and payment for purported assent by a click on a computer screen during installation. Only the largest or most specialized transactions will involve assent after negotiation.

The American Law Institute should not abandon its balanced compromise view of what is objectively manifested by blanket assent, a view adopted in the Restatement (Second) of Contracts. Blanket assent to a standard form is "to the type of transaction." Section 211, comment c. The Restatement explains, "Although customers typically adhere to standardized agreements and are bound by them without even appearing to know the standard terms in detail, they are not bound to unknown terms which are beyond the range of reasonable

expectation." Id. at comment f. In a commercial world dependent on form contracts, at least two forms of checks are needed: (1) pre-transaction availability of terms to permit shopping, and (2) a doctrine to make bizarre or oppressive terms unenforceable. A third section below discusses several other, although not all, assent problems in Article 2B.

1. Pre-transaction availability of terms

Pre-transaction availability of terms reduces the costs of shopping for the best terms and makes market competition possible. If terms are presented after purchase, the only way to shop for the best terms is to make multiple purchases and return products that come with objectionable terms, a costly proposition that impedes competition. In addition to the time involved, the purchaser may already feel committed to the deal, having ordered and paid and in some instances waited for delivery. If terms were available pre-contract, it would be possible for reporters for computer or other periodicals to gather them and publicize who is offering the best terms. While it is true that there is competition in many aspects of the software market, it is not so clear that the industry is as yet interested in competing on the basis of contingent terms involving quality assurance and remedies. It is to be hoped that the industry will evolve in the direction of warranty competition, making it inadvisable to codify current practices that may stand in the way of that goal.

Post-purchase terms are troublesome under contract law. If a contract has already been formed, as in an Internet or telephone purchase directly between the producer and the end-user, there is no consideration for the new terms. Modern contract doctrine makes modifications enforceable without consideration in some circumstances but requires a change in circumstances not anticipated by the parties at the outset of the transaction. The Restatement, in Section 89(a), makes modifications binding without consideration "if the modification is fair and equitable in view of circumstances not anticipated by the parties when the contract was made...." See also Article 2, Section 2-209, c. 2. ("'[G]ood faith' ... may in some situations require an objectively demonstrable reason for seeking a modification.") Thus, modification does not fit the situation where the software producer plans from the outset to present terms post-purchase.

Conditional assent or manipulation of when acceptance occurs are other possible doctrinal ways to attempt to make terms enforceable even though delivered after order and payment. However, software producers often do not use these techniques because they want the customer to feel that a deal has already been made. Article 2B would not require licensors to communicate at the time a transaction is entered into that the terms have not yet been presented. The Article 2B drafting committee should investigate new pro-competitive approaches that take advantage of the communicative power of computer technology. This would be in keeping with the admonition of the White House Report on Global Electronic Commerce not to carry existing law unthinkingly on to the Internet. Technology could be used to attempt to better communicate terms, rather than to obscure them. For example, in an on-line transaction, there is no reason a seller of goods or licensor of software cannot present the terms before an order is made. To facilitate shopping in general, terms could be available at Web sites.

To the extent that terms are now presented post-transaction, using "shrinkwrap" or "click through" contracts or similar methods, sellers or licensors who are well-advised by counsel know that it is doubtful that the terms are enforceable. Codifying the validity of this practice as a means to impose any term, unless unconscionable, would constitute a major shift in the balance in software transactions. Software licensors, by means of a simple "click" during installation, could routinely get all of the following: warranty disclaimers, remedy limitations, choice of law, choice of forum, prohibitions on reverse engineering and criticism, and future changes clauses. Something more meaningful in the way of assent is essential.

2. Policing Bizarre or Oppressive Terms

The Restatement (Second) of Contracts in Section 211(3) recognizes a modest limit on blanket assent to standardized contracts. As explained in comment c to that section, the drafter may be tempted to overreach. The assent that a customer gives is blanket, but as comment f points out, that should not reasonably be interpreted as giving the drafter a blank check. Under comment f, the limit on form terms is that they not be "bizarre or oppressive" or eviscerate terms explicitly agreed to or eliminate the dominant purpose of the transaction. The doctrine of reasonable expectations is closely related to the policy against unconscionable terms and the rule of interpretation of contracts against drafters. Id. at comment f.

The reasonable expectations doctrine of the Restatement has been incorporated into the UNIDROIT Principles for International Commercial Contracts, Article 2.20, (principles for commercial, not consumer, contracts). The unenforceability of unfair terms is generally recognized in Europe, Japan and many other legal systems. Article 2B will have no chance of achieving the goal of serving as a model for global software and electronic commerce if it hews to a narrow and fictional view that blanket assent means assent even to unfair terms. As of last summer the doctrine of reasonable expectations was included in the Article 2B draft (for mass-market contracts). The Drafting Committee for Article 2B voted to eliminate it last September, while the Revised Article 2 Drafting Committee continues to work on codifying the doctrine at least for consumer transactions. Neither the Restatement nor the UNIDROIT Principles restrict the doctrine to consumer or mass-market contracts.

3. Other Issues

A. Allowing one who drafts a contract to define what "manifests assent." Allowing one party, the drafter, to define objectivity is a perversion of the objective theory of contract, yet Article 2B-111(a)(2) does just that by stating that the drafter may designate conduct or operations as manifesting assent. In addition to allowing drafters to set forth what actions will manifest assent, the Reporter's Notes to Section 2B-111 recognize as sufficient devices to manifest assent, ones that a drafter might specify: (a) opening of shrinkwrap, and (b) clicking on a screen with an undisplayed license. There is reason to question whether these are adequate formalities to carry with them the idea of assent, particularly blanket assent to a long license when not in the context of a bargain, but rather in the context of supposed post-purchase validation of terms. In the Statute of Frauds, contract law has treated signing a writing as of particular significance as a formality. See also Restatement Section 211(1), referring to signing a writing as a clear case of manifestation of assent (subject to the reasonable expectations doctrine). Adoption of a digital signature in an electronic record ought to be given equal significance, but clicking--something computer users often do hundreds of times a day--is much less significant than using a code or identifying symbol pre-designated as a means of authentication.

Under contract law, oral bargain is also treated as a sufficient formality for formation. But opening a package or clicking on a computer screen after a bargain has been entered into does not necessarily satisfy the functions of a formality identified by Lon Fuller (the cautionary, evidentiary and "channeling" functions, the last meaning a device that parties know courts will treat as significant). It would be easy for a user of software to fail to understand that opening a package or clicking a computer screen has legal effect, and questions about the agency of the one opening or clicking could undercut the evidentiary function (does it matter if an employee without actual authority or your six-year-old child did the opening or the clicking?) Especially in the business context, issues concerning the agency of installing technicians would undercut the supposed certainty of the Draft's approach.

B. Validating "Future Changes" Clauses. Section 2B-304(b) permits a drafter to put into a license a term permitting future changes in the terms, so long as notice is given at the time of the change, but without the need for the other party's further assent. (Although the section uses the term "modification," this is a misleading characterization, because true modifications require mutual assent at the time of the change.) Under Section 2B-304(b), a term authorizing future changes need not be called to the attention of an adhering party or separately assented to. In mass-market contracts, Article 2B requires that the non-drafter have a right to terminate the contract at the time a change is made, but only if the change deals with a material term. Thus, a nonmaterial change that a party objects to comes in and the objecting party cannot terminate. In a nonmass-market contract, a party who "manifests assent" to a license with a future changes clause does not have a right to terminate even if a material change is made. Could the drafter increase the rate for future use, without giving the other party a right to terminate? It seems the answer is yes. The fact that someone agreed to such a "future changes" clause, without limitation to nonmaterial or advantageous changes, seems to be good evidence that the clause was not read or understood.

Only in nonmass-market licenses are material changes binding, without right to terminate as to future performance, under future change clauses. Should this allay concern about Section 2B-304(b)? The definition of a mass-market transaction in Section 2B-102(31) does not include many transactions that in common understanding might be considered mass-market ones. For example, a solo dentist who signed up for an on-line dental reference service for $50 a month for two years would not be engaging in a mass-market transaction because dental reference services are not marketed to "the general public as a whole." Thus, a dentist entering into such a license could be subject to higher charges (say, increasing the fee per month to $75) without the right to cancel the contract.

The idea of a category broader than "consumer contract" is in general a good one, to reflect that many non-consumers are as unsophisticated and as unlikely to be represented by counsel as consumers (or as likely to have too little at stake to make it worth while to use a lawyer when making the transaction or dealing with a dispute). However, the way the "mass-market" category is used in Article 2B is to give mass-market licensees the "default" rights that all buyers of goods have under Article 2, at most, and to give nonmass-market licensees less. The definition of mass-market transaction and the use of this concept in Article 2B need further attention.

Conclusion

The assent provisions in the current Article 2B draft would have a synergistic effect, amounting to a delegation of regulatory power to licensors who draft form contracts. The American Law Institute should ask the Drafting Committee to engage in fundamental rethinking to achieve a more balanced policy position on basic contract law issues.

Appendix H

Ed Foster's Gripe Line column of April 21, 2000

Downloaded from http://www.infoworld.com

Friday, Apr. 21, 2000 1:01 pm PT
The Gripe Line by Ed Foster

Maryland Legislature caves to UCITA, but Iowa may offer a safe haven from law

ON OCT. 1, THE Uniform Computer Information Transaction Act (UCITA) will become law in Maryland. IT managers, you'd better begin preparing your defenses now. In fact, you might want to build an anti-UCITA bomb shelter.

Although totally outgunned by the deep pockets of the software lobby, the anti-UCITA forces, headed up by 4Cite (For a Competitive Information and Technology Economy, the anti-UCITA coalition to which InfoWorld belongs), did a heroic job of fighting against the bill while it was debated in the Maryland Legislature. And enough Maryland legislators got the message that several amendments to significantly defang UCITA were given consideration, particularly in the Senate.

The law approved by both houses, however, contains mostly cosmetic changes while leaving all the dangerous stuff untouched. You might have heard that Maryland's version of UCITA protects consumers against defective software by not allowing vendors to disclaim the implied warranty. That would be a significant change if it weren't for UCITA's narrow definition of a consumer: It applies only to those who acquire a product "primarily for personal, family, or household purposes" and specifically not for "professional or commercial purposes." Unless you buy a word processor only to write letters to Aunt Jane, it's not a consumer transaction under Maryland's UCITA and you're out of luck if the product doesn't work.

Another "fix" in Maryland's UCITA that doesn't help in the real world is an amendment to the notorious electronic self-help provision that says the right to disable software products remotely cannot be exercised in "mass-market transactions." Mass market is another term in UCITA that sounds good but is actually so oddly defined that it might not mean anything at all. (A New Jersey legislative commission, after studying the UCITA reporter's comment on mass-market transactions, noted that "In light of the comment, it would appear that the purchase of a single shrink-wrapped copy of Microsoft Office at a mass-market retail outlet such as Staples or OfficeMax by a four-person law firm would not fall within the UCITA definition of a 'mass market transaction.' ") You can bet, though, that IT purchases of any sort don't come under any

mass-market protections.

Maryland's electronic self-help fix fails on another count as well. It prevents vendors from exercising self-help in a mass-market transaction, but it doesn't prevent them from including a remote disabling mechanism in a mass-market product. The distinction is important, because it's highly unlikely anyone actually will follow UCITA's formal rules for exercising electronic self-help. What is more likely is that vendors will include backdoors and time bombs for anti-piracy or other purposes. Should a customer discover that the remote disabling capability is there -- perhaps after suffering a disaster due to it being triggered accidentally -- UCITA protects the vendor from liability.

This brings me to the first and most important defensive measure every IT organization should take to prepare for a world where UCITA exists even in a few states: Starting now, demand that vendors warrant that their products are not self-help capable. Make that demand a critical part of your software procurement process. According to some readers, not only are many corporations doing just that, but several government agencies are also considering revisions to their procurement practices. This isn't surprising, particularly in the case of organizations for critical infrastructures. The possibility that any software inside the firewall could have unknown self-help mechanisms raises enormous security issues. Corporations and agencies that don't start asking vendors very pointed questions will soon be guilty of a dereliction of duty.

Electronic self-help is just the most scary item on the list of UCITA horrors. I'm beginning to compile examples from readers of anti-UCITA defense tactics, which I'll share at a later date. In the meantime, there is one thing you can push for in your state that could protect everyone against UCITA.

Several concerned corporations in Iowa have helped promote what has been called bomb-shelter legislation to protect all Iowa customers, consumers, and businesses from UCITA or UCITA-like laws in other states.

The bomb-shelter law says that a transaction between an Iowa party and a party that tries to invoke the law of a UCITA state will instead be subject to the laws of Iowa -- a fine example of Midwestern common sense, if you ask me. An amendment to this effect was passed by the Iowa House as part of its Electronic Transaction Act (HF 2205) and now awaits consideration by the Senate. Software industry lobbyists are swarming into the state like angry mosquitoes. Perhaps some of the common sense that has been lacking on either shore of the Potomac will be found in more abundance in the Midwest

Appendix I
Ed Foster's Gripe Line column of August 25, 2000
Downloaded from http://www.infoworld.com

Friday, Aug. 18, 2000 1:01 pm PT
The Gripe Line by |Ed Foster

UCITA lets vendors reach in and disable your software, forcing you to upgrade it

IN CASE YOU HAVEN'T already noticed, let me point out an interesting connection between spyware and the Uniform Computer Information Transactions Act (UCITA). Intrusive software might not be there just to snoop: Under UCITA it can be there to legally disable your software when the vendor wants to force you to buy the next version.

You didn't know vendors could leverage UCITA to force customers to upgrade? I have to apologize for that, because only recently have I come to realize that UCITA's "automatic restraints" provision makes this a likelihood for shrink-wrapped software products. I have a good excuse, though: The tangled mess that is UCITA still has surprises for even the most careful of students.

And as long as I'm apologizing, let me take this opportunity to announce that we have finally brought our UCITA section on InfoWorld.com (www.infoworld.com/UCITA) up-to-date. We'll be adding more material to it in the next few months and will endeavor to do a better job of keeping it current. I could try to point fingers elsewhere, but it's my fault it has been so long. The only quasilegitimate excuse I have here is that I do get tired of writing about this thing, as much as many of you get tired of reading about it. Unfortunately, it's necessary.

By the way, there is an excellent site that anyone interested in tracking UCITA should check out: IEEE-USA's UCITA Grassroots Network page at www.ieeeusa.org/grassroots/ucita/index.html. The Institute for Electrical and Electronics Engineers has taken a strong stand against UCITA, and the site contains valuable resources, position papers, and state-by-state tracking of the legislation. In my humble opinion, the opposition to UCITA by IEEE, the Association for Computing Machinery, and other groups representing technical professionals is the most telling evidence that the law is bad not just for customers but for the software industry itself.

In fact, I have to suspect the automatic restraints concept is one of main reasons the big software companies are pushing so hard for UCITA. On the surface, the provision (Section 605 in UCITA parlance) looks fairly innocuous, at least compared to the blatantly controversial

Section 816 about electronic self-help that's been the focus of so much attention. A quick reading would give you the impression that the restraints 605 talks about are only such things as metering software that limits access to the number of licensed users or time bombs in demo software to restrict how long the program can be used. A closer look reveals more.

"Licensees generally have no problem with the type of compliance tools that the term 'automatic restraints' leads one to imagine," says Elaine McDonald, assistant director for corporate purchasing at The Principal Financial Group. "But the definition in UCITA does not really require the restraint to be automatic; in fact, it clearly doesn't exclude a restraint that is intentionally triggered by the vendor at a time of their choosing. In other words, it is possible for a vendor acting under Section 605 to exercise what amounts to electronic self-help without even the minimal protections provided under Section 816."

There is an "or" in Section 605 that's easy to miss. In describing situations where vendors can enforce a usage limitation with an automatic restraint, UCITA says it can be done if a term of the agreement authorizes its use, if the restraint prevents use that is inconsistent with the agreement, if the restraint prevents use after a state duration or state number of uses, or if the restraint prevents use after one party notifies the other the agreement is being terminated. In other words, the user has done nothing wrong, nothing in the agreement allows for use of the restraint or says that time is up, and the licensor can still turn off the software by giving "reasonable notice." (As you know from our sneak-wrap discussions, that means no real notice at all.)

UCITA is full of "terminate-at-will" language that says either party can end a license agreement when they wish unless there is a stated duration for the contract. I've urged IT managers to make sure that their negotiated contracts specify they have perpetual rights to software. But it's a rare shrink-wrap or click-wrap license that grants perpetual rights. There is a very weak presumption of a perpetual license in some cases under UCITA, but it's easily overcome by vendors that design their licenses with the intent of using automatic restraints.

UCITA says the license on a shrink-wrapped product runs out when the vendor chooses, and the first you might know of it is when you find the program's no longer there. And if a bug or hacker triggers the restraint, UCITA protects the vendor there, too. Be it intentional or accidental, if an automatic restraint wipes out your software -- even wipes out your company -- under UCITA you'll have no recourse against the vendor who slipped the software onto your system. I bet the spyware makers can hardly wait.