

## Melissa's Message

If you've spent the last several months in the Galapagos Islands, you may not have heard of the Melissa virus. As the rest of us now know, Melissa is designed to let itself replicate exponentially by exploiting the ability of Microsoft Word to run macro attachments, a known security risk. While Melissa caused some sites to disconnect themselves from the Net, significantly slowed down other sites, and created a lot of grief for systems administrators, its effects could have been a lot worse. Melissa hit near the end of the business day on a Friday, and, although it disabled virus checking and generated large amounts of unwanted email, it appears no disks were trashed or files overwritten.

What, if anything, can policy makers learn from Melissa? Will they take steps to make computers, software, and the Net more secure and robust? Or will they pass laws that are likely to encourage buggy software and irresponsible business practices?

Because state laws govern commercial transactions in the U.S., the Uniform Commercial Code (UCC) was developed as a way to facilitate interstate commerce. Most of the UCC is law in all 50 states; Article 2, which applies to the sale of software, is law in 49 states. Article 2B<sup>1</sup> will apply to contracts involving digitized and other kinds of intellectual property. It will formalize in law many current shrink-wrap license provisions, some of which are likely to encourage the marketing of non-robust, buggy software.

Anyone who has written a large program realizes it's impossible to produce bug-free code and extremely difficult to produce robust and secure software. Consequently, we don't hold software producers liable for every bug in their programs. But that doesn't mean they should be absolved of all responsibility for any problems that might occur because of their software. UCC2B would make it trivially easy for software producers to limit their

liability to only the purchase price of the software, even if the producer knew the software contained serious bugs at the time of sale. It's a bit like telling food processing companies that if they knowingly sell contaminated food, they are required to refund only the product's purchase price to people who became ill by eating it. If this aspect of UCC2B becomes law, it could place companies that strive to produce relatively bug-free and secure code at a disadvantage when competing with less-professional companies. This is hardly a good strategy for developing a secure Net.

Benchmarking practices are another problem confronting software developers and users. Companies have been known to tailor their products to optimize benchmark performance. Yet when benchmarks are customized for a set of tests, there is the risk the benchmarks might, intentionally or inadvertently, favor some of the software being tested over other software. In spite of the known problems of benchmarks, they are used as a rough method for comparing software and hardware. UCC2B, if approved, will exacerbate the problem of evaluating and comparing software by legitimizing nondisclosure agreements. In other words, if you want to compare, say, several different database programs, you may need the permission of each of the database companies to publish your results. Presumably, companies whose software did not perform especially well would be unlikely to allow you to publish information about their software. This rule applies not only to benchmarks, but also to any kind of software analysis, assuming the analysis is based on having run the software.

Consequently, software producers, unlike most producers, would be given considerable control over what is said about their products. At a time when information about insecure products should be publicized, we may find ourselves forbidden by law from doing it.

Other portions of UCC2B place the consumer at a disadvantage. For example, a consumer probably could not hold a producer liable for statements included in the manual unless the consumer saw

<sup>1</sup>In April 1999, Article 2B was renamed the Uniform Computer Information Transactions Act (UCITA) and removed from the UCC. UCITA will probably be introduced in the state legislatures unless it is first blocked at a Denver meeting scheduled for July.

## • From the President

the manual prior to the sale. By contrast, the software producer would not be required to make a copy of the license or any warranty disclaimer available for the customer to read prior to purchase. The consumer's only recourse would be to return the software if he or she objects to the terms, which are frequently made known to the consumer only during installation of the software.

### What Should We Do?

Cem Kaner and Todd Paglia, lawyers who focus on software quality, have proposed an alternative approach to UCC2B. (A detailed description of the problems associated with UCC2B can be found on Kaner's Web site: [www.badsoftware.com](http://www.badsoftware.com).) They recommend that software producers should be free from liability for damages caused by any defect that:

- Was not known to the producer at the time the publisher sold the product, provided the lack of knowledge was not due to grossly negligent development or testing practices; or
- Was described in material accompanying the

product, written in a way a typical member of the product's intended market could understand.

Otherwise, either the defect was known but not documented, or the quality control was drastically inadequate. There are differing views about whether there should be a cap on economic damages recoverable due to defects in mass-market software. This and related liability questions have underlying technical aspects the legal community is not equipped to evaluate unaided. Computing professionals should be involved in any such debate, and should insist that any laws adopted encourage the development of sound, robust, and secure software.

We have constructed a large and complex system in which potential security problems are frequently ignored. Transforming the information infrastructure into a robust system will not be easy. We must focus on policies and laws that encourage, rather than discourage, the goal of a safe and secure information infrastructure. ■

BARBARA SIMONS ([president@acm.org](mailto:president@acm.org)) is ACM's president.

### Index to advertisers

Advertiser	URL	Email	Phone/Fax	Page
AAAI-99	<a href="http://www.aaai.org">www.aaai.org</a>	<a href="mailto:ncai@aaai.org">ncai@aaai.org</a>	650-328-3123	14
Bond University	<a href="http://www.bond.edu.au/bondit/">www.bond.edu.au/bondit/</a>		142	
Charles River Analytics			fax 617-868-0780	139
City University of Hong Kong	<a href="http://www.cityu.edu.hk">www.cityu.edu.hk</a>	<a href="mailto:hrmail@ctylnk.cityu.edu.hk">hrmail@ctylnk.cityu.edu.hk</a>	fax 852-2788-1154	142
Dice Recruitment	<a href="http://www.dice.com">www.dice.com</a>			143
EPFL	<a href="http://www.epfl.ch">www.epfl.ch</a>		fax +41 21 693 70 84	58
EPFL	<a href="http://www.epfl.ch">www.epfl.ch</a>		fax +41 21 693 70 84	143
Information Resources	<a href="http://www.infores.com">www.infores.com</a>	<a href="mailto:irirec@infores.com">irirec@infores.com</a>	fax 312 627 4279	137
Kaplan	<a href="http://www.Kaplan.Careers.com">www.Kaplan.Careers.com</a>		888-265-6972	92
MIT	<a href="http://web.mit.edu/personnel/www/resume.htm">web.mit.edu/personnel/www/resume.htm</a>			141
North Carolina State University	<a href="http://www.csc.ncsu.edu">www.csc.ncsu.edu</a>			13
Panasonic				138
SAC 2000	<a href="http://www.acm.org/conferences/sac/sac2000">www.acm.org/conferences/sac/sac2000</a>			135
SIGIR '99	<a href="http://www.sims.berkeley.edu/conferences/sigir99">www.sims.berkeley.edu/conferences/sigir99</a>			66
Smith College	<a href="http://www.smith.edu">www.smith.edu</a>			137
Syddansk Universitet				140
Tech expo	<a href="http://www.tech-expo.com">www.tech-expo.com</a>			CIV
University of Pennsylvania				141
Career Opportunities				136-143

For further information regarding product and recruitment advertising call the representative in your area:

**ACM Headquarters** +1-212-626-0685 [andrzejewski@acm.org](mailto:andrzejewski@acm.org)

**Southeast** Walter Andrzejewski +1-212-626-0685, [andrzejewski@acm.org](mailto:andrzejewski@acm.org)

**West** Marshall Rubin & Associates +1-818-995-8828 [mrubin@westworld.com](mailto:mrubin@westworld.com)

**Midwest/Texas** Bart Engels +1-847-854-6050 [engels1@aol.com](mailto:engels1@aol.com)

**Northeast/NY/NJ/PA** The Summit Group +1-908-876-1249 [hersh@ibm.net](mailto:hersh@ibm.net)