UCITA (4): Action
by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

The previous three articles in this series have reviewed the Uniform Computer Information Transactions Act (UCITA) and common arguments for and against this model legislation. This article presents a nightmare scenario based on UCITA.

***

It is the year 2006. Jamal is the network manager for a company with 10,000 PCs running Fenestration YQ2, an older version of the Fenestration operating system (the current version Fenestration YQ4). In 2003, Mocraherd, the software supplier, changed the terms of the software license so that each license expires after one year; to renew the license, Jamal's company has to pay a renewal fee -- or the operating system shuts down for good and the company has to purchase completely new licenses at a higher price. Now Mocraherd has told Jamal that he is required to upgrade to YQ5 within the next couple of months or lose his corporate licenses altogether.

The problem is that the new Fenestration YQ5 that's being advertised requires over 2 GB of free disc space for the operating system upgrade and a minimum of 512MB of RAM plus a 2.0 GHz processor as minimum configurations -- and upgrading the company's computers would cost at least $500 each. Including the cost of upgrading to YQ5 ($50 per system), that makes a total cost of around $5,500,000 -- not including the cost of labor and downtime. Worse still, reports in the underground press (it's a violation of license to publish or read any material that is critical of Mocraherd or Fenestration version using Mocraherd products) indicate that the new YP version takes four hours to install, fails in a third of the installations, and does not support the type of printer, external removable hard drives, or scanners that Jamal has installed on half his systems.

Jamal's options are limited. He knows that Fenestration YQ2 includes spyware that automatically reports on the states of all machines where it has been installed; he knows because in several cases, changing defective mother boards on some downed PCs resulted in complete shutdown of the operating system. Jamal's staff had to call Mocraherd and get permission to reactivate the OS using a new license code. Then all the installed Mocraherd products stopped working, so his staff spent hours on the phone to Mocraherd waiting for new activation codes for each computer. Jamal tried stopping the spyware from reaching the Internet using personal firewalls as well as the corporate firewall, but the Macroherd software eventually shut down when it could no longer receive encrypted continued-operation codes from Mocraherd.

Unfortunately, Jamal's staff consists of only 50 support staff for the 10,000 computers in the network; he simply does not see how they are going to install updates to all the computers in the company in a reasonable time. Worse still, the new Fenestration YQ5 OS does not run the old version of the Officious product suite (Verb word processor, Punctuate display software, Crunch spreadsheet and Excess database) and files created with the new version of the Officious suite are not usable by the old Officious products.
Jamal decides to investigate alternatives to running Mocraherd programs altogether. He scans a few articles online about possible competitors using the Mocraherd Internet Exploder browser; as far as he can see, the costs of conversion would be prohibitive and the range of programs is inadequate to replace the Mocraherd programs. In addition, ever since Mocraherd started suing companies for making their products and file formats interoperable with those used by the software giant, competing companies are withdrawing products and going bankrupt.

An hour later, he receives a legal writ via e-mail warning him that he has violated the terms of his software license by accessing sites which are hostile to the interests of Mocraherd. Then his computer shuts down due to a remote signal from the Mocraherd Web site. Because the corporate license covers all the computers in the company, all the other computers shut down within minutes too. Finally, the electrical power, telephone, and HVAC (heating, ventilation and air-conditioning) computers shut down too even though all of them are running on separate licenses of Fenestration YQ2. No matter: an error in the programming on the Macroherd servers automatically assumes that all computers that are colocated are on the same license.

Jamal waits in the dark and wonders what to do next.

* * *

From the license for FrontPage 2002: "'You may not use the Software in connection with any site that disparages Microsoft, MSN, MSNBC, Expedia, or their products or services . . . ' the license reads in part." -- Ed Foster, "A punitive puppeteer?" <http://www.infoworld.com/articles/op/xml/01/09/17/010917opfoster.xml>

Windows Update checks the Microsoft site every five minutes and alerts users when critical updates are available; in order to tell if such updates are required, each system reports on its configuration so the server process can tell if it needs changes. This process cannot be stopped once it starts (short of uninstalling the product). The Microsoft Knowledge Base confirms that no user intervention is permitted: "Question: Can I change the scheduled behavior of Windows Critical Update Notification? Answer: No, if the scheduled task is modified, the tool reverts to the default settings the next time Windows Critical Update Notification runs. Note that this behavior is by design to ensure that you are notified of updates in a timely manner." <http://support.microsoft.com/support/kb/articles/Q224/4/20.ASP>

* * *

Whether what you have read so far about UCITA pleases you or horrifies you, go do your own research to see if this legislation will protect you and your corporate interests. Then contact your state law-makers to let them know your stand on this approach to contract law.

You already know my opinion. Now go make up your own minds.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations
management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.