Comment on DMCA "anti-reverse-engineering" provisions.

As a frequent user of software for the past two decades, I have often come across programs with performance at variance with their advertised claims.

When a non-software manufacturer produces a product that doesn't do what it is supposed to, you can generally find where the product is failing, taking it apart if needed, and demand that it be fixed or that the product be removed from the market. In extreme cases, the manufacturer can be prosecuted for fraud or false advertising.

The DMCA gives makers of software an extraordinary shield against exposure of fraudulent practices: anyone that reverse-engineers their software and comments publicly is liable to be sued into silence, using the DMCA.

This is not mere speculation; there is currently a court injunction on the authors of a program that decrypts the blocking list of a web-filtering program (cf. MICROSYSTEMS SOFTWARE vs. SCANDINAVIA ONLINE). The decryption program was not to evade the filtering software, but rather to show what the software is doing, by allowing users to see the "blocked URLs list". Note that MICROSYSTEMS does not own these URLs, they have simply compiled and categorized them (sometimes erroneously) and applied a simple encryption to the list.

There has been a long history (http://www.peacefire.org/) of the makers of web-filtering software blocking sites in error, and the response of these software manufacturers to having their errors pointed out has ranged from the disingenuous to the outright fraudulent or libelous, such as labelling detractors as "pornography".

The DCMA's "anti-reverse-engineering" provisions hands such manufacturers a big stick to silence their critics. I'm sure the auto manufacturers of 30 years ago (and today!) would love to have a similar law to use against Ralph Nader, the Consumer's Union, and anyone else that dares to contest their claims.

We do not license and restrict photocopiers, although they can very easily be used to circumvent copyright, because they can be used for other useful purposes as well. Reverse engineering also can be used to provide interoperability (still protected under DCMA) and also to show and repair the deficiencies of a consumer product. As our society depends more and more on software, it is critical that citizens be able to examine those products and to comment freely on their findings.

Under prior copyright laws, such reverse-engineering and commentary would be protected under "fair use" and "research and education" provisions, as they should be. We need to be free to read, to examine, and to comment and criticize.

Copyright is about rewarding authors to enhance communication. The DCMA's anti-reverse-engineering provisions are about stifling communication to reward media giants. Those provisions have no place in a free society.

--

Charles Lane, Assoc. Prof.
Physics Dept.
Drexel University
Philadelphia PA 19104

215/895-1545 lane@duphy4.physics.drexel.edu