Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The DMCA Still Restricts Forensics

In about 2000 I stopped making ForensiX available because, as software for digital forensics, it bypassed normally effective protection measures to gain access to content on computers. Of course this is something that many sorts of forensic software mechanisms do, but as far as I am aware, the competitors in the market have just ignored the law. Comes 2010, and the Library of Congress, charged with rulemaking has made the ruling at right – at least as of now...

C. Software and information recorded, produced, stored, manipulated or delivered by the software, that a forensic investigator seeks to copy, activate, or reverse engineer in order to obtain evidence in a court proceeding.

Glenn Pannenborg proposed designating a class of works for the benefit of forensic investigators (*i.e.*, court–appointed evidence examiners) seeking evidence in a court proceeding. According to Pannenborg, forensic examiners practicing in the fields of financial or information technology may be faced with evidence that is recorded, produced, stored, manipulated or delivered by software covered under 17 U.S.C. 1201, or evidence that may be the software itself, as in a patent or licensing dispute. He asserted that in order to obtain access to such evidence, a forensic investigator may have to circumvent a technological protection measure in violation of Section 1201(a)(1)(A).

Joint Creators opposed Pannenborg's proposal, and NTIA has advised the Register that it believes the record does not support granting the request.

The Register finds that the proponent in this case has not met the statutory burden of proof. Pannenborg failed to intelligibly describe the nature of authorship of the proposed class of works. Moreover, he presented no compelling evidence, and provides no concrete examples, that noninfringing uses of works in the proposed class have been or will be affected by the circumvention ban. Indeed, he provided little information about the works to which he has apparently been denied access. Because of the lack of such information in the record, an evaluation of whether and the extent to which the prohibition on circumvention caused an adverse effect on noninfringing uses was not possible. The Register, therefore, declines to recommend that the Librarian designate this proposed class of works.

What does this mean?

It seems to me to mean that any mechanism that a private examiner (law enforcement was exempted by statute) uses that has the effects of bypassing a normally effective protection mechanism (e.g., the user ID and password on Windows and protection settings on a file or directory) is no longer an open question, but rather, is unquestionably a violation of the law as it stands.

Use any such tool in your investigation, and you violate the DMCA. This is, of course, problematic for investigating not only computer-related crimes, but also traces in civil cases. Here are some examples you might be interested in:

- If you extract a mailbox file from a disk and it wasn't originally protected to allow your access, you cannot parse, examine, read, or work in any way with it's content without violating the DMCA, because such files are normally effectively protected. It's not that it is hard to examine the file – it's that normally, you can't read the content, so by reading it, you are defeating normally effective protection.
- If you get a Microsoft Word document, you cannot look inside it to determine the meta-data associated with its components, because it is not normally available to the user at the Microsoft interface. It's not that we don't have the tools to do it – it's because you have to reverse engineer to do it – or buy and use a product that defeats the, normally effective, protection of those copyrighted contents.

A note on copyrights

To gain clarity around this issue, it is worth noting that, due to changes in the copyright law over time, any work that is realized in any documentary form; be it a recording, computer file, hand written on a piece of paper, cut in wood, etched in silicon, or you name it; is de-facto copyrighted. There are some exceptions for government documents and certain types of public records, but other than that, when you write an email to your sibling, it is a copyrighted work and subject to the laws regarding copyright – including the DMCA.

There are some really good things about that. It used to be that to enforce a copyright you had to send a copy to the Library of Congress and mark all copies (like this document is marked). But that's no longer true, and as a result, minor mistakes don't cause your copyrights to be invalidated. That's a benefit, and one that I have taken advantage of by not having to continue to pay copyright fees like I used to have to do whenever I wrote anything that I cared about.

But as usual, it's the unintended consequences that get us... or are they now intended consequences?!?

The implications of this ruling

If those in the digital forensics business actually bothered to try to obey the laws, this would mean that no company could even access its own files if they were protected by even something as simple as a password, because, again, it violates the DMCA. And it also means that the vast majority of commercial tools violate the DMCA. If your tool makes copies of files on disks, whole disks, extracts meta-data from file systems, etc., without going through the normal user interface of the host system, which may alter the content and thus the evidence. This is because you are accessing copyrighted works that have normally effective protection.

While companies like Encase, FTK, and others have long gotten away with the excuse that they sell to law enforcement – or that the law wasn't explicit in this area – this is no longer the case. While the next round of rulings is scheduled for about 3 years from now, in the meanwhile, there can be little doubt now that these sorts of tools and their use is violative.

But will the courts follow the law and rulings here?

In my view, it's bad public policy for courts to ignore laws and rulings from Federal agencies legally responsible to make such rulings. But then I am not a judge, and I don't have to balance the needs of the justice system against ... the needs of the justice system. I suspect that no case will be overturned, that no evidence will be thrown out, that no forensics tool makers will stop producing tools, and that the only companies and people who will end up harmed are those who follow the laws and rules.

Will any Federal judges read this? I doubt it. Will State and Local judges apply the ruling to stop evidence from getting in? I don't think so. Will the inequity between the prosecution and the defense be recognized? After all, the prosecution is exempt from the DMCA in its search for evidence, while the defense in its quest for material evidence ignores the law at its own peril. Or will all defendants and civil parties have to ask each judge for permission to do this each time for each case? Will judges place orders to force or allow this?

What will you do? Ignore the law? Or not help your clients as well as you might?

