BEFORE THE COPYRIGHT OFFICE LIBRARY OF CONGRESS

IN THE MATTER OF EXEMPTION TO THE PROHIBITION OF CIRCUMVENTION OFCOPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROLTECHNOLOGIES

Docket No. RM 2005-11

Comments of Glenn Pannenborg, CPA

Pursuant to the Notice of Inquiry (NOI) and request for comments issued by the United States Copyright Office (the Office) published in the Federal Register at 70 Fed. Reg. 57,526 (Oct. 3, 2005), I submit the following comments with respect to the Copyright Office's triennial rulemaking establishing temporary exemptions to the federal prohibition on circumvention of copyright protection systems for access control technologies.

1. Proposed classes of works

Computer software

2. Summary

This comment proposes an exemption to 17 U.S.C. 1201 Circumvention of Copyright Protection Systems for Forensic Investigators. The subparagraphs herein identify who or what a Forensic Investigator is, how the trade of Forensic Investigator is affected and restricted by 17 U.S.C. 1201, the adverse effect of said restriction to the forensic investigator, attorneys, law enforcement, civil regulators and the public at large, and the limitations of existing exceptions and alternative methods in mitigating those restrictions.

3. What is a Forensic Investigator

Forensic investigators may practice in a wide variety of technological or scientific fields. For the purposes of this comment the term is narrowed to apply to forensic investigators practicing in the fields of financial or information technology as these are the fields impacted by 17 U.S.C. 1201.

The business of a forensic investigator is to examine evidence in a civil or criminal proceeding and to issue a report thereon to a court. Forensic investigators may be employed by civil attorneys, defense attorneys, prosecutors, law enforcement, civil regulatory agencies or directly by a court.

Forensic investigators may present a variety of credentials to support their qualification to practice their trade. These include academic degrees, industry certifications, or public licenses among others. But they are ultimately accredited by the scrutiny and evaluation of the relevant court. Any party to a legal matter or the court itself may challenge the forensic investigators qualifications.

4. Activities of a forensic investigator restricted by 17 U.S.C. 1201.

Forensic investigators examine evidence and report thereon. The evidence may take the form of information that is recorded, produced, stored, manipulated or delivered by software covered under 17 U.S.C. 1201. Alternatively evidence may be the software itself, as in a patent or licensing dispute.

In the case where the evidence to be examined is the software itself the interaction of investigator and software is self-evident.

In the case where the evidence is information recorded, produced, stored, manipulated or delivered by the software:

a) Evidence may be encrypted by the software, either for security or compression, in such a way that only the software itself or a detailed knowledge of the software's program can translate the data.

b) Evidence may extend beyond the information input to or output from the software. This evidence may take the form of knowledge of the internal functions of the software such as the timing of events that produced the data or the capabilities and restrictions of the software in manipulating data. A good example would be questioning whether the software allows data to be altered after it is entered and, if so, does it leave a record of when and by whom.

In any of the above scenarios it may be incumbent on the investigator to copy, activate, or reverse engineer the software in order to acquire the required evidence. All actions that may, without specific authorization from the copyright holder, violate the provisions of 17 U.S.C. 1201.

5. Adverse impact of restrictions placed on a forensic investigator by 17 U.S.C. 1201

Incomplete or inaccessible evidence impacts the rights of litigants and criminal defendants to due process. Likewise restrictions that limit acquisition of evidence hinder the ability of law enforcement and civil regulators to conduct investigations and prosecutions necessary for public safety.

I can attest to two investigations where I proposed to attorney clients that software be acquired by means of a motion for discovery. In both cases the situation was substantially identical. Evidence was available in both paper document and electronically readable records. The electronic records contained data that was not present on the

documents and that the software had no function to produce. That electronic data was encrypted in an unknown compression format making it unreadable without access to the software.

In both cases the opposing attorneys made informal objections on the grounds that

a) their client would be in violation of their copyright agreement with the software manufacturer and
b) that the request lacked relevance because the installation media allowed only one installation and was unusable without circumvention of the digital protection.

The first point is moot for this commentary as it relates to other aspects of copyright law. But the second argument demonstrates the restriction imposed by 17 U.S.C. 1201. My client could not reasonably argue to the court that the software was relevant because we did intend to circumvent the copyright protection in violation of 17 U.S.C. 1201. Due to the legal obstacles involved, no formal motion was made and my reports were issued with specifically identified gaps.

6. Limitations of established exceptions

Sections 1201(e) and 1201(j) provide exceptions for “Law enforcement, intelligence, and other government activities” and other parties respectively to be exempted for “security testing”. There is no exemption for civil or criminal investigation.

Section 1201(g) provides an exemption for “Encryption research”. While some portion of the restrictions described herein may very loosely fit this definition, that position is subject to challenge and the balance of issues raised remain unaddressed.

7. Limitations of other avenues for the forensic investigator

Arguments could be made that a forensic investigator can request permission from the software manufacturer and failing that seek an order from the court to compel the software manufacturer to provide information. There are situations where this is unlikely to be effective:

a) When the software manufacturer is beyond the jurisdiction of the court and chooses not to comply
b) When the software manufacturer exists as a corporate entity and copyright holder but has no staff or no individuals possessing the requisite technical knowledge to comply
c) Where the software manufacturer has a vested interest in protecting their client and may choose to render incomplete or inadequate compliance. In such case neither the court nor the forensic investigator would be in a position to evaluate whether compliance was complete or adequate.

8. Related arguments

The intent of 17 U.S.C. 1201 is to protect the rights of copyright holders. The rules for exemption focus on adverse effect of restrictions but it could be argued that an exemption that causes an adverse effect on the copyright holders could undermine the statute as a whole. In the case of this proposed exception it can be noted that forensic investigators are bound by the rules of the court for handling evidence in a secure and confidential manner and are ultimately under the authority and observation of the court issuing the original order. As such, the proposed exemption places the copyright holder under little or no risk.

Respectfully Submitted

/S/
_____
Glenn Pannenborg
Gelnn Pannenborg, CPA, PC
1 Congress Street, Suite #A7
Jersey City, NJ 07307
(201) 984-4554