Paula J. Bruening
Office of Chief Counsel
National Telecommunications and
Information Administration
Room 4713
U.S. Department of Commerce
14th and Constitution Avenue, N.W.
Washington, D.C. 20230

Jesse M. Feder
Office of Policy and International Affairs
U.S. Copyright Office
Copyright GC/I&R
P.O. Box 70400, Southwest Station
Washington, D.C. 20024

Re: Request for Comments on Section 1201(g) of the Digital Millennium Copyright Act, Docket No. 990428110-9110-01

Dear Ms. Bruening & Mr. Feder:

As professionals working in data security and encryption, we wish to comment on the "expert exception" of the Digital Millennium Copyright Act. In general, we believe that the DMCA together with the "expert exception" will be very detrimental to the general interests of the American public, individuals and businesses alike. Specifically, as an integral part of the DMCA, we feel the "expert exception" will not provide assistance in combating illegal copying and other breaks, but instead will act as a shield for inappropriate and bad security and actually promote undesired exploits.

The expert exception allows for professionals, academics, and licensees with consent of the content owners to analyze the cryptography of the products or technology. Others are restricted from doing so, except under a small set of conditions. Further, the dissemination of any information regarding weaknesses of a system is restricted to the same group of interested parties. While well intended, there are troubling aspects to this: Without broadening this exception, the likely consequence will be a weakening of the overall strength and quality of the products that are brought to market. The licensees of technology will be less certain of the consequence of using that technology and put at far more jeopardy than before the act with the "exception" were made into law. The reliance on consent as a requirement for licensees to examine technology is unreliable and inappropriate when considered for cryptographic examination and testing. These points are examined immediately below.

First, regarding who can challenge. It is in everyone's interest to examine cryptographic and security systems as widely as possible. Any problems with a system will be found eventually. It is simple, better sooner than later. It is simply necessary to provide a wide opportunity of analysis to the whole community of computer professionals, content

providers, prospective licensees and others just to gain satisfaction about the relative protection of systems used by users. After all, the protection of all parties involved is what is at stake here. Cryptography used in a system should be thoroughly examined for the same reason cars go through crashing tests, with results available to the consumers. Cryptography is no longer a research topic, it is rather a technology used in a wide variety of commercial systems. The overall protection that a licensee can expect from a vendor cannot be evaluated always from a single work or even a selected body of works that they have access to. Instead, the strength of the cryptography and security will be from the entire body of materials and technology suites that use the technology. Giving the right to challenge to a small number of testers on a selected amount of material may not provide enough exposure to all the potential problems to provide confidence to any of the parties.

The security industry as a whole condemns "security through obscurity" as ineffective. Obscurity in a system is ultimately analyzed and the problems with it seen. What was obscure, if important becomes widely analyzed and quite open. The security of a system is as good as the number of qualified and interested people who have examined the system. The crux of the matter is "against whom are you protecting?" Bad guys will examine it no matter what. You just can't stop it. It is far better to all the interested parties to allow everyone to look at cryptography right off the bat. The real protection of intellectual property comes from the copyright law, rather than from the encryption that prevents its easy copying; the quality of the encryption must stand on its own regardless of who is trying to break it. Real security is built on technology that works, regardless of who knows about it. Content owners must understand level of security that technology provides. All content providers simply cannot employ enough security professionals to analyze and attack copyright encryption schemes (especially small ones!). It is impossible for them to examine all the potential uses of systems and applications that might expose any problems. There must be a recognition that the open analysis and sharing of information in the broad commercial and academic communities is necessary to protect all parties interests in matters related to copyrighted material.

There is a saying in the industry, "no security is better than weak security". Weak security has a number of bad consequences. It provides essentially no protection, it introduces cost for consumer and producer, and it hides problems. With the new act and the restrictions of the "exception", this latter problem becomes enormous. In fact, claiming to have security without doing the required due diligence can be easily positioned as "deception" from the consumer standpoint and could be litigated as knowingly marketing and selling products without doing the best to ensure proper functionality. Providing any statement to consumers regarding the functionality of the product is not valid without proper examination, publicly.

The exception attempts to restrict the actual testing to parties that have connections to the technology in question. Besides professionals and academics, these are direct licensees of the technology, and then only if they have the consent of the relevant copyright holder. This is simply not the way technology is tested and evaluated these days for licensing or adoption. Especially in the case of communications systems, openness is crucial. A

vendor's choice of encryption technology actually affects the entire industry. The failure of even one vendor to establish and choose the appropriate encryption technology can have wide spread effects on the entire industry. It is no longer the case that commercial interests are served directly by academic pursuits. A viable technology needs to be tested and serviced by the actual community of users. This restriction is just setting up for an enormous failure.

There is a false belief that "cryptography" lives in a vacuum. Like many parts of technology, cryptography is utilized as a component in increasingly complex systems. Encryption is now a basic component of many operating systems, hardware platforms, and application software. It is not only the security expert but also computer system engineers and quality engineers who need to certify and examine the technology. As such, testing the entire system must include certain tests of the correctness and robustness of the encryption subsystem. With this exception as written, such tests may actually be in violation of the proposed law. This merging of unencrypted and encrypted data is probably going to be the most significant change to the nature of systems over the next few years. The discipline of maintaining an environment that can actually be trusted is a requirement for the U.S. industry to lead as it has.

The question even arises as to who this exception will actually benefit. It seems obvious that most interested parties benefit more from a wider body of testers than the exception allows. Potential licensees of a technology need to know whether they can trust the security of the system or not. It is a huge undertaking to decide on and implement a technological solution. If they can't submit it to arbitrary tests, they can't make an intelligent decision. Take a silly case, where all data of a product is encrypted with a minimal key, say 1 byte. But the producer may represent it as secure. According to this act, anyone who intentionally tested the security if not for research or directly established commercial interested would be in violation. But, any attacker would go after the key and it would happen rapidly using available cryptanalysis tools. The protection in that environment is afforded to the attackers rather than the content producers or the licensees of the technology. The licensee and original technology providers are both losers. Consumers lose when technology is unavailable or flawed. Only competitors or hackers seem to be victorious.

In conclusion, though there is no question that the issue of copyright protection is a serious one that needs significant legislative attention, the "expert exception" hurts the overall effort of development and protection of intellectual property. As computer security and cryptography specialists we encourage a much more open and realistic approach to the problem. Ultimately, the protection of any data will depend on the overall strength of the cryptography and systems that implement the security. This should be acknowledge with an "exception" that encourages as much testing and overall cooperative development of technology as possible. Weak cryptography will always be broken. It is better to focus on the illegal use of content and corresponding enforcement rather than to limit activities that promote cryptography and technology that actually work.

Thank you very much for giving us this opportunity to comment.

Sincerely,

Taher Elgamal
President
Kroll O'Gara Information Security Group

Dan Kolkowitz
Vice President
Kroll O'Gara Information Security Group

Mark Chen
Chief Cryptographer/CTO
Kroll O'Gara Information Security Group