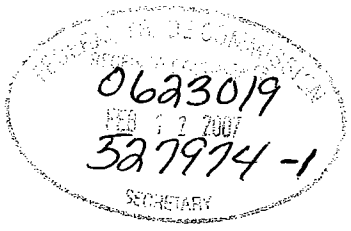

NY
31 Jan 2007

Federal Trade Commission
Office of the Secretary
Room H-135
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Gentlebeings:

I am writing to comment on the proposed settlement in the Sony BMG CD Rootkit case, FTC File No. 062-3019. To summarize my position, the settlement is wholly inadequate, and the following actions should be taken:

1) A referral should be made to the U.S. Attorney's office for criminal trespass under various federal computer statutes.
2) The FTC should file a civil complaint against Sony BMG under the various federal statutes for deceptive and misleading business practices, and seek major financial damages on behalf of every consumer affected by Sony's reckless actions.
3) The FTC should seek a permanent injunction against Sony using any kind of malware that interferes with a user making additional copies of Sony distributed CDs for their own private use.

My justification for why the settlement as it stands is inadequate (using the analysis of the consent order provided by FTC staff):

Parts I, II and III of the consent order do nothing to prohibit Sony from installing malware on users' systems, as long as Sony disclosures the use of such software, the software does not violate the provisions of Part VI, and users' consent is required to install it. I am a computer consultant, and would be someone that a user would call to fix a system infected by malware. Most users would not understand the implications of consenting to the installation of software provided by Sony. The DRM software that Sony installed on users' systems in the current case, overtly or covertly, did more than just restrict access to Sony intellectual property. It opened the systems to stealthy attacks, and those stealthy attacks materialized once the scope of Sony's DRM software was publicly revealed (see http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1144441,00.html). There is nothing in the agreement to prevent Sony from installing software that makes users' computer vulnerable to attacks from the Internet that they would otherwise not be subjected to.

While the uninstaller would presumably close any vulnerability caused by Sony's DRM software, why should a user have to choose between having a safe system, or being able to listen to a CD he bought?

Part IV of the consent order prohibits Sony from using information it has collected for any purpose, and requires Sony to destroy it. Since the information was collected by trespassing on users' systems and collected without their consent, why should Sony not pay every purchaser damages for its unlawful actions?

Part V of the consent order requires Sony to notify users if they are required to consent to information collection to listen to a CD they purchase. This requirement does not in any way prohibit Sony from collecting information; it merely requires Sony to notify users of this requirement. This requirement does not adequately protect users or serve public policy. Sony should be prohibited from collecting this information, because:

1) It has no requisite function with the playing a CD (i.e., these are separate and discrete functions, and there is technological dependency on the other; any such dependency is strictly procedural).
2) Sony is being rewarded for previous illegal behavior; the requirements of Part IV notwithstanding. Providing the required notification to users is not a burdensome requirement for Sony.
3) Merely requiring it to notify users does nothing to prevent Sony from misusing collected data.

Instead of rewarding Sony, it should be sanctioned for its previous illegal activities by being prohibited from collecting information; such a prohibition would send a powerful message to Sony.

Part VI of the consent order is a good beginning, but, as mentioned in comments on Parts I, II and III, does not require Sony to avoid methods that put users' systems at risk.

Part VII of the consent order again provides a generally good requirement on Sony, but I object to Sony being allowed to retain "counter" elements. Since existing Sony software trespassed on the users' computers in the first place, again, Sony is being rewarded for unscrupulous and blatantly illegal behavior, and denying it this ability would again send a powerful message to Sony.

Part VIII of the consent order requires Sony to provide CD exchange and repair reimbursement. These provisions are wholly inadequate:

1) There is no provision for payment for individuals who performed their own repairs.
2) The nature of the damage to computers was significant enough that $150 (equivalent to 2 to 3 hours of computer support time) is not adequate to reimburse users. Mark Russinovich, a noted Windows Expert, initially uncovered the Sony XCP controversy, and reported upon it in his blog

(http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx). He needed advanced tools and techniques beyond the reach of most computer professionals to remove the offending software and fix the system (the nature of the software is such that simply removing the software caused the CD drive to no longer be recognized by the system). Users who used (or hired someone else to use) a manual procedure to remove the software would have had to go through a similar frustrating procedure. I will also note that the consent order limits repair costs to $150, while Sony's own repair claim form puts a limit of $175 with receipts. Sony also reserves the right to limit reimbursement to $25 without receipts, which is unfair to people who did not have the presence of mind to save the receipts for future submission (at a time when any action against Sony was not even formulated), or who never obtained one in the first place, for the same reason.

3) Sony provides a number of options for replacement of CDs. However, it limits cash payments to $7.50. Since most new CDs are in the $12-$15 range, Sony should increase the cash payment to $15.

Part IX of the consent order allows Sony to continue to sell MediaMax CDs as long as it notifies users of the security issues with MediaMax and provides a download patch from a web site. I believe this is also inadequate. Users should not be required to download a patch for DRM software that Sony failed to provide adequate security or notification for initially. Again, I believe this is rewarding Sony for bad behavior, and Sony should be required to destroy ALL remaining copies of these CDs, rather than release them to the public. That would send a strong message to Sony.

In summary, the proposed consent order is insufficient to deter or punish Sony for its bad and criminal behavior. Sony will continue to issue bad DRM-encoded CDs, albeit with more disclosures, some limited restrictions, and mandated uninstallers. Other music publishers will not be deterred either from issuing bad DRM-encoded CDs, but simply learn to avoid some of the more egregious acts that Sony made. In terms of public benefit and public policy, this is simply a bad consent order that benefits Sony more than the public. For the reasons above, please reject the proposed consent order, and either negotiate a more favorable agreement that protects the public against bad DRM and punishes Sony for its ill-conceived actions (including hiding links for uninstallers and requiring users to register to download installers that caused even more vulnerabilities on users' systems), or else file criminal and civil charges against Sony. Even if the FTC does not want to pursue litigation and prosecution against Sony, the threat of such action would quickly bring it back to the negotiating table. Sony should be held accountable for its actions, and this consent agreement does NOT do that.

Sincerely,

Jeffrey Harris