

An Open Letter to Sony-BMG

To: Andrew Lack, CEO of Sony-BMG
Cc: Rolf Schmidt-Holtz, Chairman of the Board, Sony-BMG
Cc: Howard Stringer, CEO of Sony Entertainment
Cc: Gunter Thielen, CEO of Bertelsmann AG

Dear Mr. Lack,

The Electronic Frontier Foundation (EFF) has viewed with growing concern the revelations regarding the XCP Content Protection Software and the SunnComm MediaMax software that your company has chosen to include on at least two dozen of your music CD releases. We are also concerned by your company's limited response to the concerns of your customers and the computer security community.

As has been documented by independent researcher Mark Russinovich and many others, the XCP software appears to have been designed to have many of the qualities of a "rootkit." It was written with the intent of concealing its presence and operation from the owner of the computer, and once installed, elements of the software run continuously -- even when no Sony-BMG music CD is in use. It provides no clear uninstallation option. Additionally, without notifying users, the software appears to contact a remote machine under your control. The MediaMax software is somewhat different, but similarly has no true uninstall option and an undisclosed ongoing communication from the users' computer to SunnComm.

You must be aware that the discovery of this software has shocked and angered your customers. Software that deceives the owner of the computer it runs upon and opens that computer up to attacks by third parties may be expected to come from malicious cyber-attacks; it is certainly not expected nor acceptable to be distributed and sold to paying customers by a major music company. Accordingly, EFF welcomes your company's decision to temporarily halt manufacturing CDs with XCP and to reexamine "all aspects" of your "content protection initiative."

But if you truly intend to undo the harm you have caused, your company should immediately and publicly commit to the following additional measures:

- Recall all CDs that contain the XCP and SunnComm MediaMax technology. The recall must include removing all infected CDs from store shelves as well as halting all online sales of the affected merchandise. We understand from a recent New York Times article that well over 2 million infected CDs with the XCP technology are in the marketplace and have yet to be sold.
- Remove from all current and future marketing materials statements like that on <http://cp.sonybmg.com/xcp/english/updates.html> that say the cloaking software "is not malicious and does not compromise security."

- Widely publicize the potential security and other risks associated with the XCP and SunnComm MediaMax technology to allow the 2.1 million consumers who have already purchased the CDs to make informed decisions regarding their use of those CDs. The publicity campaign should include, at a minimum, issuing a public statement describing the risks and listing every Sony CD, DVD or other product that contains XCP or SunnComm MediaMax. The publicity campaign should be advertised in a manner reasonably calculated to reach all consumers who have purchased the products, in all markets where the CDs have been sold.
- Cooperate fully with any interested manufacturer of anti-virus, anti-spyware, or similar computer security tools to facilitate the identification and complete removal of XCP and SunnComm MediaMax from the computers of those infected. In particular, Sony should publicly waive any claims it may have for investigation or removal of these tools under the Digital Millennium Copyright Act (DMCA) and any similar laws.
- Offer to refund the purchase price of infected CDs or, at the consumer's election, provide a replacement CD that does not contain the XCP or SunnComm technology. For those consumers who choose to retain infected CDs, develop and make widely available a software update that will allow consumers to easily uninstall the technology without losing the ability to play the CD on their computers. In addition, consumers should not be required to reveal any personally identifying information to Sony in order to access the update, as Sony is currently requiring.
- Compensate consumers for any damage to their computers caused by the infected products, including the time, effort, and expenditure required to remedy the damage or verify that their computer systems or networks were or were not altered or damaged by XCP or SunnComm MediaMax products.
- Prior to releasing any future product containing DRM technology, thoroughly test the software to determine the existence of any security risks or other possible damages the technology might cause to any user's computer.
- Certify in a statement included in the packaging of every CD containing DRM technology that the product does not contain any concealed software such as the XCP rootkit, does not electronically communicate with Sony-BMG or any other party, does not initiate the download of any software update or other data without informed consent of the consumer immediately prior to each communication, can be uninstalled without any need to contact Sony or disclose personally identifying information to anyone, does not present any security risks to any consumer's computer, and will not damage or reduce the performance of the consumer's computer or data in any way.

We look forward to hearing that you are in the process of implementing these measures by 9:00am PST on Friday, November 18, 2005.

Sincerely,

Electronic Frontier Foundation