

January 2006

## Sony-BMG Copy Protection Rootkit

Berkeley Technology Law Journal

Follow this and additional works at: <https://scholarship.law.berkeley.edu/btlj>

---

### Recommended Citation

Berkeley Technology Law Journal, *Sony-BMG Copy Protection Rootkit*, 21 BERKELEY TECH. L.J. 551 (2006).

### Link to publisher version (DOI)

<https://doi.org/10.15779/Z38R96H>

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Technology Law Journal by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact [jcera@law.berkeley.edu](mailto:jcera@law.berkeley.edu).

## ADDITIONAL DEVELOPMENTS—CYBERLAW

### *SONY-BMG COPY PROTECTION ROOTKIT*

In October 2005, security researchers discovered that Sony-BMG was distributing a controversial form of copy protection on millions of its music CDs, prompting strong reactions from the technical and public interest communities as well as state law enforcement officials, ultimately leading to a series of investigations and lawsuits.

Sony-BMG, a record company and music distributor, is one of the largest firms in the industry. Last year it was discovered that several million of its music CDs were protected by XCP, a copy protection technology that restricts the ability of users to copy and access music on their computers. In order to prevent users from removing this software, XCP employed a rootkit—a cloaking technology that hides files from users and their operating systems. Because rootkits enable third parties to surreptitiously install software on users' computers, Sony-BMG's undisclosed installation of such technology on their customers' machines sparked a great deal of concern from consumer rights groups and security professionals who claimed that Sony-BMG was engaging in "black hat hacking" and deceptive trade practices.

Sony-BMG's response to the concerns was unsteady at best. While it released a series of programs to allow users to uninstall XCP's rootkit, these fixes created additional security risks. Criticism peaked when Thomas Hesse, president of Sony-BMG's Global Digital Business, stated on National Public Radio: "Most people, I think, don't even know what a rootkit is, so why should they care about it?"

In November, the Electronic Frontier Foundation filed a class action lawsuit on behalf of customers affected by Sony-BMG's copy protection. The lawsuit settled out of court, with Sony-BMG agreeing to make clear to users what type of copy protection a CD uses, and to give affected consumers a new, copy-protection-free CD, DRM-free music downloads, and a small compensatory payment. In addition, the Texas Attorney General filed charges against Sony-BMG for violating the state's anti-spyware law. Litigation and additional investigations in this matter are ongoing.

**UPDATE ON  
SHRINKWRAP/CLICKWRAP/BROWSEWRAP CONTRACTS**

***JAMES V. MCDONALD'S CORP.***

*417 F.3d 672 (7th Cir. 2005)*

***HUBBERT V. DELL CORP.***

*835 N.E.2d 113 (Ill. App. Ct. 2005)*

***MOTISE V. AMERICA ONLINE, INC.***

*346 F. Supp. 2d 563 (S.D.N.Y. 2004)*

***REGISTER.COM, INC. V. VERIO, INC.***

*356 F.3d 393 (2d Cir. 2004)*

***CAIRO, INC. V. CROSSMEDIA SERVICES, INC.***

*2005 U.S. Dist. LEXIS 8450 (N.D. Cal. Apr. 1, 2005)*

Several recent cases examined the legal significance of unconventional forms of contract formation. In each case, a court held the parties were contractually bound. The effect of these rulings is to expand the law governing the acceptance of contract terms in the shrinkwrap, clickwrap, browsewrap, and related contexts.

In *James v. McDonald's Corp.*, the Seventh Circuit addressed the validity of contract terms that are neither read by, nor immediately communicated to a contracting party, but are published and available to both parties. McDonald's promoted a game in which purchasers of food products also received the chance to win prizes. The plaintiff obtained a game card when she purchased an order of French fries. After a dispute regarding her entitlement to a prize, she filed suit, alleging that McDonald's misrepresented the true chance of winning. McDonald's filed a motion to compel James to arbitrate her claims under the contest rules posted at participating McDonald's restaurants.

The district court granted McDonald's motion to compel arbitration, and the Seventh Circuit affirmed. The court held that the arbitration clause found in the "Official Rules" was part of the contract and therefore binding. In reaching this decision, the court relied on the fact that the contest rules were posted and referred to on the packaging James received with

her game card. James contended that she should not be required to arbitrate her claims because she never entered into an agreement to arbitrate her dispute. The court disagreed, reasoning that even though the plaintiff did not read the rules in their entirety, she agreed to be bound by them by participating in the game.

In *Hubbert v. Dell Corp.*, the plaintiffs bought computers from Dell over the internet. Each of the online forms the buyers completed contained a hyperlink to the "Terms and Conditions of Sale." These terms included an arbitration clause. Dell filed a motion to compel arbitration. The trial court denied the motion, finding that the arbitration clause never became part of the contract. Dell appealed.

The Illinois Court of Appeals determined that the trial court erred in holding that the arbitration clause was not effective. The court reasoned that the blue hyperlinks constituted sufficient notice to the plaintiffs and, therefore, the terms were binding. The court noted that the hyperlink appeared on several webpages the plaintiffs necessarily viewed while ordering their products, as well as on the defendant's marketing pages. The court likened the five-step online process to a multi-page, written paper contract. As with a traditional paper contract, the Terms and Conditions were part of the contract, and the plaintiffs were bound by the arbitration clause within them.

In *Motise v. America Online, Inc.*, a New York federal court ruled on the application of an Internet Service Provider's (ISP) contract terms to an individual who was not party to the original contract, but used the ISP's service. Plaintiff used his stepfather's America Online (AOL) account to access the internet. Plaintiff filed suit, alleging that AOL released private information about him on a public listserv. AOL responded by seeking to either dismiss the action or, alternatively, transfer the case to the Eastern District of Virginia as provided by the forum selection clause in the AOL member agreement. The plaintiff argued that he did not receive notice of AOL's Terms of Service and so was not bound by them. AOL countered that (1) the plaintiff received constructive notice through availability of the terms and notice on the initial webpage and (2) the plaintiff was a sub-licensee of his stepfather.

The court rejected AOL's constructive notice arguments and instead reasoned that because the plaintiff was able to utilize AOL's services through his stepfather's account, he accepted the terms of service as a sub-licensee. The forum selection clause was therefore enforceable. The plaintiff's stepfather was required to accept the terms of service and was therefore bound at the time he created the account. When accessing the internet through his stepfather's account, the plaintiff was subject to the same con-

ditions and limits on privileges as the original licensee, his stepfather. Thus, the court reasoned that contract enforcement must extend to users of an ISP even in cases where those users did not receive actual or constructive notice of the terms of service.

Two recent cases extended contract enforcement to instances where acceptance was automated, and additional terms appeared via hyperlink only after the party had assented to the transaction. These cases mark a further departure from the standard doctrine where an offeree accepts with the benefit of full knowledge of the terms and conditions of the contract. As with *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), the landmark shrinkwrap case, the courts in *Register.com, Inc. v. Verio, Inc.* and *Cairo, Inc. v. Crossmedia Services* held that under some circumstances ex post awareness of contract terms was sufficient to bind a party. The courts extended contract enforcement to those cases where parties repeatedly and systematically utilized the websites at issue, and thus were made aware of the additional terms of use.

In *Register.com, Inc. v. Verio, Inc.* the Second Circuit heard an appeal from a preliminary injunction granted by the district court. Register.com was appointed a registrar of domain-names by the Internet Corporation for Assigned Names and Numbers (ICANN). Under its agreement with ICANN, Register.com was to make contact information for domain-name owners called "WHOIS information" available to the public. Verio was engaged in the business of selling a variety of website design and operation services. Verio used an automated program to collect WHOIS information from Register.com's WHOIS database on a daily basis. Subsequent to each receipt of information from Register.com's database, Verio also received terms prohibiting the use of the information for mass commercial e-mail, telemarketing, and direct mail. With the contact information for domain-name owners in hand, Verio solicited potential customers via e-mail, telephone, and direct mail. Though this practice violated the terms accompanying the WHOIS information, Verio claimed that because the terms were supplied only after delivery of WHOIS information it was not bound by the restrictions.

The Second Circuit affirmed the grant of a preliminary injunction. The court reasoned that Verio's argument might have been persuasive if its use of the WHOIS information had not been so frequent and systematic. Since Verio used the service on a daily basis, it received repeated notice of the restrictions against mass unsolicited e-mail. Verio admitted to knowing of the restrictions, yet continued regardless.

The facts and reasoning in *Cairo, Inc. v. Crossmedia Services* mirrored those in *Register.com*. Cairo filed a federal suit in California seeking a de-

claratory judgment that it did not breach any contract with the defendant, Crossmedia Services (CMS). Cairo's website allowed a user to search its database of retail sales information. To provide such information, Cairo used a software robot to automatically collect sales information from the various retailers' webpages. CMS, one such retailer, authorized users to view and download a single copy of content on its website solely for lawful, noncommercial and personal use. Its terms of use also contained a forum selection clause. These restrictions were made available from CMS's home page via a hyperlink labeled "Terms of Use." Cairo's computer search programs could not "read" the Terms of Use, and they did not report the presence of such terms back to Cairo. Cairo asserted that since it used a robot and never explicitly agreed to CMS's "Terms of Use," it was not contractually bound by the forum selection provision.

The district court granted the defendant's motion to dismiss Cairo's suit. The court in *Cairo* concluded that because Cairo's use of CMS websites, although automated, was performed thousands of times per month, knowledge of CMS's terms of use could be imputed to Cairo. Thus, even accepting Cairo's assertion that it did not explicitly agree to the Terms of Use and forum selection clause, its use of CMS's websites created actual or imputed knowledge of CMS's terms of use and bound Cairo to those terms.