

Firm Tracking Users of Pharmaceutical Websites Wins Privacy Lawsuit

September 2002

On August 13, 2002, a Massachusetts federal district court granted summary judgment in favor of Pharmatrak, the defendant in an online privacy class action. *In re Pharmatrak, Inc. Privacy Litigation*, Civil Action No. 00-11672-JLT, MDL Docket No. 1400 (D. Ma. August 13, 2002). The court rejected claims that Pharmatrak's undisclosed monitoring of website users violated federal privacy laws, largely following the reasoning of similar web tracking decisions regarding DoubleClick, *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497 (S.D.N.Y. 2001), and Avenue A, *Chance v. Avenue A Inc.*, 165 F.Supp.2d 1153 (W.D. Wash. 2001). These cases indicate that federal courts are looking with skepticism on challenges to web monitoring raised under federal privacy laws.

Cookies and Web Bugs

Pharmatrak was hired by several major pharmaceutical companies to monitor how their websites were being used. Pharmatrak placed cookies on users' hard drives and used "web bugs" on the pharmaceutical websites to track users without their knowledge. These technologies allowed Pharmatrak to monitor where consumers went on the sites, the length of time users spent on each webpage, and what sites the users had visited immediately prior to coming to the pharmaceutical websites. Pharmatrak advised the pharmaceutical companies that it did not collect personally identifiable information. However, the plaintiffs alleged that Pharmatrak occasionally received some personally identifiable information incidental to the site-usage data it collected.

Class Action Complaints

In August 2000, plaintiffs filed class action lawsuits against Pharmatrak and its pharmaceutical company customers in federal district courts in Massachusetts and New York. The complaints alleged violations of the federal Electronic Communications Privacy Act ("ECPA") and the Computer Fraud and Abuse Act ("CFAA"), in addition to state-law claims. Shortly after these lawsuits were filed, Pharmatrak went out of business. However, the lawsuits proceeded and were consolidated in Massachusetts federal district court.

No Violation of ECPA

The district court held that Pharmatrak's activities did not violate ECPA. Title I of ECPA prohibits the interception of electronic communications in transit when the interception is (1) unauthorized or (2) authorized, but done with the intention of committing a tort or a crime. Title II of ECPA prohibits unauthorized access to

electronic communications stored in a facility used to provide communications services.

The plaintiffs first claimed that Pharmatrak intercepted communications in transit between users and the pharmaceutical websites. The pharmaceutical companies clearly authorized Pharmatrak to intercept such communications. However, the plaintiffs argued that this authorization did not extend to Pharmatrak's interception of personally identifiable information. The court rejected this distinction. As in *DoubleClick* and *Avenue A*, the website operators' consent to intercept communications was all that ECPA required, even if the website operators did not fully understand the operation of the technologies used to collect information. Further, the court found no indication that Pharmatrak intercepted the communications with the *intent* of committing a tort or a crime, even though the plaintiffs alleged that torts had been committed. Thus, Pharmatrak's monitoring did not violate Title I of ECPA.

Nor did the information collection violate Title II. First, the court found that individual users' computers are not the type of facilities protected by ECPA. While some personal computers can perform the "server-like" functions used to provide Internet access service, there was no evidence that the plaintiffs used their computers in that manner. Further, as under Title I, the court held that Pharmatrak's access was authorized by the pharmaceutical companies. Finally, citing *DoubleClick*, the court held that ECPA's Title II is intended to protect only electronic communications being stored temporarily, incident to their transmission. The cookies storing information on users' computers thus did not fall within the scope of Title II.

No Violation of CFAA

The court also rejected the plaintiffs' CFAA claims. Among other things, the CFAA prohibits the unauthorized access of a protected computer to obtain information. However, civil claims only are available to parties that suffer damages of "at least \$5,000 in value during any 1-year period" "by reason of a violation" of the CFAA. The court agreed with *DoubleClick* and *Avenue A* that the \$5,000 threshold must result from a "single act" of unauthorized access to a computer. The plaintiffs had no evidence that the online monitoring caused at least \$5,000 in damage through a single act, even when aggregated over any 1-year period. Thus, the plaintiffs could not recover under the CFAA.

Other Remedies?

After dismissing the three federal claims, the court declined to exercise its supplemental jurisdiction over the plaintiffs' state-law claims, dismissing those claims without prejudice.

The *Pharmatrak*, *DoubleClick*, and *Avenue A* decisions seem to indicate that federal privacy statutes offer little support for class action plaintiffs' counsel seeking to challenge online monitoring through cookies and similar technologies. It remains to be seen whether these plaintiffs will have more success with their state-law challenges, or whether such plaintiffs will seek to have web monitoring addressed more directly, through new federal or state privacy laws.

For additional information, please contact Bruce L. McDonald (202.719.7014 or).