Courts Find that Online Profiling Is Legal

2002-11-08

Recent court cases have improved the legal status of online profiling, a controversial practice described in our Internet Alert of August 28, 2000 in which web site traffic and users' Internet browsing patterns are tracked by third parties. Online profiling companies, advertisers, Internet Service Providers and web site operators may now be more inclined to expand their use of online profiling technologies.

In the latest victory for online profiling companies, the U.S. District Court for Massachusetts rejected claims that Pharmatrak, Inc., an Internet marketing data provider, and five of its pharmaceutical company clients violated federal wiretapping, privacy and computer fraud statutes. Seven individual plaintiffs alleged that Pharmatrak accessed their hard drives, recorded their interactions with certain web sites by means of cookies and other methods, and obtained sensitive personally identifiable information without sufficient consent.

Pharmatrak contracted with its pharmaceutical company clients to monitor user activity on those clients' web sites to track web page traffic, information about medical conditions and pharmaceutical product sales. The agreements between Pharmatrak and its clients provided that Pharmatrak would not collect "personally identifiable information." In light of the nature of the information amassed by Pharmatrak, the plaintiffs argued that Pharmatrak clients did not authorize the data collection.

The plaintiffs alleged that Pharmatrak collected data about users' web browsing and information submitted through online registration forms, search queries and email transmissions. Pharmatrak also used small data files, or cookies, to store this tracking data on users' hard drives. The plaintiffs alleged that these methods enabled Pharmatrak to obtain users' names and addresses, telephone numbers, birth dates, insurance information, information about medical conditions, education history and employment information.

The plaintiffs brought claims under several federal laws, including: Title I of the Electronic Communication Privacy Act of 1986, also known as the Wiretap Act; Title II of the Electronic Communication Privacy Act of 1986, also known as the Stored Wire and Electronic Communications and Transactional Records Act; and the Computer Fraud and Abuse Act.

- The Wiretap Act generally prohibits non-law enforcement personnel from intentionally intercepting electronic communications, but permits certain interceptions if there is no criminal purpose and one of the parties to the communication has given consent. The *Pharmatrak* court concluded that there was no Wiretap Act violation upon finding that Pharmatrak's clients had consented through their contracts with Pharmatrak and that Pharmatrak had no criminal intent. The court observed that "it is irrelevant for the purposes of the Wiretap Act whether the Pharmatrak clients knew the precise mechanisms of Pharmatrak's service or not."

- The Stored Wire and Electronic Communications and Transactional Records Act prohibits intentional, unauthorized access of a "facility through which an electronic communication service is provided" in order to access stored electronic communications. Although the Pharmatrak court acknowledged that the law was intended to prohibit computer hacking, it found that the Internet services used by the plaintiffs - not the plaintiffs' personal computers - were the "facilities" protected by the law. The court also found that Pharmatrak's clients provided sufficient authorization for the data collection services.

- The Computer Fraud and Abuse Act prohibits the intentional, unauthorized access of a computer to obtain information in connection with an interstate communication, involving an aggregate loss of at least $5,000. The *Pharmatrak* court found that the plaintiffs failed to show how the alleged privacy violations caused the monetary damage needed to trigger the law and, therefore, did not need to discuss the substance of the plaintiffs' privacy claims.

The privacy protections afforded under the Health Insurance Portability and Accountability Act ("HIPAA") would not have been at issue in the *Pharmatrak* case, because those rules will apply only to individually identifiable health information handled by health plans, health care providers and health care clearinghouses, or business associates acting on their behalf. For further discussions of HIPAA and its implementing regulations, see our Internet Alerts of November 2, 1999, May 31, 2001 and October 4, 2002.

The *Pharmatrak* case, as well as another recent decision, have made it more difficult to challenge web site monitoring and online profiling, but highlight the importance of adequately disclosing to the sources of the data how the information will be collected and used. For a discussion of privacy protections recommended for the online profiling industry, see our Internet Alert of August 28, 2000, which discussed the Network Advertising Initiative guidelines, an industry-driven set of privacy principles that was endorsed by the Federal Trade Commission in 2000.

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089