

# World Media Law Report

This printed article may not be photocopied and is for the exclusive use of Ms Michelle Mancino Marsh. For a multi-user licence please contact Alan Mowat on +44 20 7234 0606.

June 05 2008 - USA

Kenyon & Kenyon LLP

## New Jersey court broadens constitutional right to privacy

In a unanimous decision in *State v Reid* the New Jersey Supreme Court has extended the right of privacy to cover information stored by an individual's internet service provider (ISP) regarding his or her internet activity.



James E Rosini

The state of New Jersey sought an indictment of an employee for second-degree computer theft by maliciously changing her employer's access codes to the employer's supplier's website. Tracking the intruder's internet protocol (IP) address back to the ISP that assigned it, the state sought to subpoena the ISP's records to learn the identity of the intruder.

IP addresses are assigned to individual users by ISPs, which keep records of assigned IP addresses. Thus, the only way to correlate the identity of a user to an IP address is to obtain such information from the ISP.

The New Jersey Supreme Court held that the state had improperly sought the identity of the intruder by serving a faulty subpoena on the defendant's ISP. It agreed with the defendant that such an improper subpoena violated her right of privacy, holding that users have a reasonable expectation of privacy when surfing the Internet privately at home.

Traditionally, federal courts have not extended privacy rights to cover information exposed to a third party by an individual (eg, *Smith v Maryland* granted no right of privacy regarding dialled telephone numbers; in *United States v Miller* the court found no right of privacy regarding bank records). However, recently some states, including New Jersey, have been willing to accord broader privacy protection than is provided by the Fourth Amendment. For example, previously the New Jersey Supreme Court expanded the expectation of privacy to cover telephone billing records held by the telephone company (*State v Hunt*, 91 NJ 338, 347 (1982)). Expanding on this, in the case at hand the New Jersey Supreme Court noted that disclosure of IP address information to an ISP is required solely to facilitate online surfing, and a user has a right to protect this surfing activity from unreasonable searches and seizures, even if that information is held by the third-party ISP (*slip op* at 16).

However, the court noted that as technology develops, it may be possible to trace IP address activity directly back to a user without requiring private information held by an ISP. If that occurs, users may no longer have a reasonable expectation that such information will be kept private (*id* at 21).

Finally, although the subpoena was faulty, the court held that a proper grand jury subpoena could acquire the IP address information. A grand jury's expansive investigative powers allow it to conduct discrete inquiries without the normal requirements of probable cause or notice to the individual being investigated (*id* at 23-24). As the information was obtained from the business records of a third-party ISP, there was no indication that such information was tainted by virtue of the faulty subpoena, and thus could be reacquired through proper means.

It would seem that as long as ISPs continue to act as a bulwark for users' internet activity, at least some states will recognize a limited right of privacy subject to proper search and seizure means.

James E Rosini, Michelle Mancino Marsh and Erik Kane, Kenyon & Kenyon LLP, New York

© Copyright 2004 - 2008  
Globe Business Publishing Ltd