

This story came as the result of a breaking news pitch. Within hours the interview was secured, completed, and sent to press.



## Supreme Court Justice's social security number stolen, posted on LimeWire

**By Byron Acohido**  
**USA TODAY**

Warning: using your workplace PC to log onto your favorite [peer-to-peer](#), or P2P, service can be extremely hazardous. Just ask Supreme Court Justice Stephen G. Breyer.

His social security number was among 2,000 stolen from investment firm Wagner Resource Group, and subsequently discovered free for the taking on music-sharing site LimeWire, says the [Washington Post](#).

It seems one of Wagner's employees accessed LimeWire from a work computer, and introducing a data-stealing program into the company's network.

The firm should have had a policy prohibiting use of LimeWire on company computers, says Phil Neray, VP at database security company

[Guardium](#). But Wagner Resource really doesn't deserve to be singled out. Untold numbers of organizations are open to data-stealing attacks delivered via popular P2P services -- any company that permits employees to use free instant messaging services at work, for instance.

"Companies have a long way to go, and the bad guys know it," says Neray. "The bad guys will continue mining peer-to-peer networks for sensitive data as long as organizations keep their heads in the sand about internal and external threats"

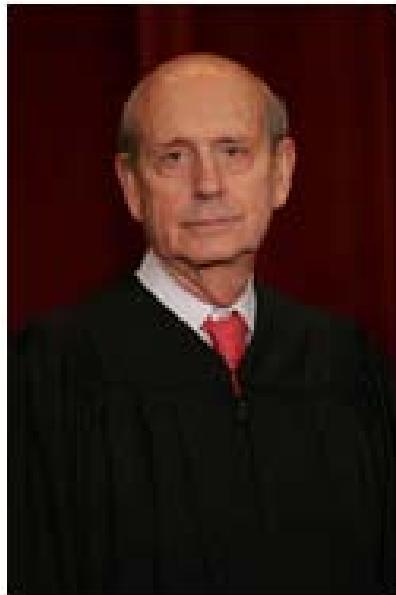


Photo: Breyer  
(Tim Dillon, USA TODAY)