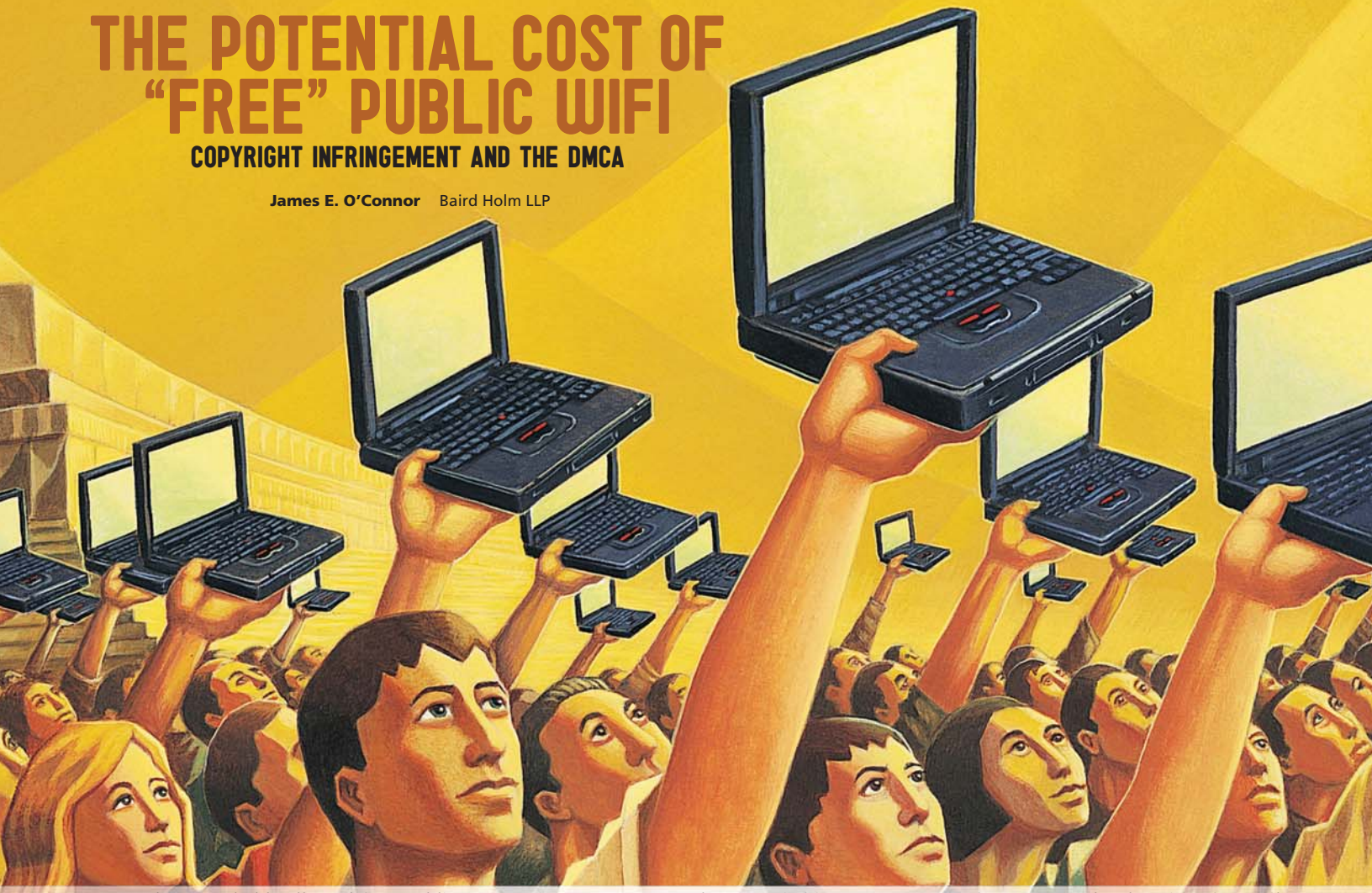
THE POTENTIAL COST OF "FREE" PUBLIC WIFI

COPYRIGHT INFRINGEMENT AND THE DMCA

James E. O'Connor Baird Holm LLP



We have probably all used free public WiFi to access the Internet at a coffee shop, lunch or when visiting a bank, hospital, hotel, or other business. While free public WiFi access to the Internet is convenient for customers, it is not without substantial risk to the business offering such access. Some individuals may use the free access to carry out infringing activities – such as downloading movies from an illegal file-sharing site, "swapping" songs through a music sharing service, or pirating software. These infringing activities on the part of customers can potentially leave businesses vulnerable to claims of copyright infringement and subject to both civil and criminal liability. However, businesses can protect themselves from potential copyright liability by taking proper proactive measures which will be addressed later in this article.

AVENUES OF LIABILITY

Under copyright law, there are four avenues of liability for copyright infringement, which may apply to public WiFi providers:

1. Direct infringement occurs when an individual actually carries out the infringing act. For example, a user infringes a copyright when he downloads a movie or song without permission from the copyright owner. WiFi providers are not liable under direct infringement unless they or their employees/agents are the ones carrying out the infringing act.

2. Contributory infringement occurs "by intentionally inducing or encouraging direct infringement." This definition comes from *MGM v. Grokster*, where the Supreme Court held a peer-to-peer file sharing software company liable for contributory infringement because its services were known to encourage copyright infringement activities.

3. Vicarious infringement occurs when an individual or entity profits from direct infringement, while the entity maintains the ability to stop or control the infringement. The factors of vicarious liability also come from *Grokster*, where the Supreme Court determined that Grokster profited from its infringing software and had the ability to stop the infringement by cutting off access to its software. How the theories of contributory and vicarious infringement apply to providers of free public WiFi will remain for the courts to decide.

4. The final avenue of liability for WiFi providers for copyright infringement arises under a theory of negligence. Under this theory, it is negligent for WiFi providers to leave their network open and unsecured, knowing that other individuals may connect and engage in infringing activities. The concept of negligence has not traditionally been applied to copyright infringement law, and the courts will ultimately decide whether this approach will be adopted. However, in light of this possibility, it is prudent for WiFi providers to consider proactive measures to shield themselves from liability.

INDUSTRY ENFORCEMENT TACTICS

With the advent of peer-to-peer file sharing, infringement of music and movies has increased exponentially, and copyright owners have implemented new enforcement tactics. For example, over the last 13

years, the Recording Industry Association of America ("RIAA"), has pursued lawsuits against various parties with the objective of targeting the "key" parties in the infringement chain to reduce the overall level of infringement. In 1999, the RIAA began suing the peer-to-peer file sharing networks, including Napster, Grokster and their equivalents, in an attempt to target the source of the infringement. But the ease of creating a peer-to-peer network has prevailed, and new file sharing sites appear continuously. So these suits did not make a considerable impact on infringing activities. In 2003, the RIAA began pursuing individual infringers. As of early 2006, the number of total suits against individual infringers totaled 17,587.[1] Intensifying the attack on individual infringers, the RIAA began pursuing college students by contacting universities to have them forward pre-litigation infringement notices to the students whose IP addresses were identified as engaging in infringing activity. In 2008, at the height of this campaign, the RIAA had sent over 5,400 of these letters. However, none of these tactics appears to have considerably reduced infringing activities.

More recently, copyright owners have targeted the next link in the infringement chain, namely, Internet Service Providers ("ISPs"). The copyright owners have negotiated with ISPs so that the ISPs will forward copyright infringement notices to individual subscribers. The goal of this program is to prevent future infringement, first through education, and if necessary, mitigation measures.

The process works as follows: 1) a copyright owner monitors the Internet for infringing content and identifies the IP addresses where infringing material is found and the IP addresses that access it; 2) the owner notifies the corresponding ISP, who will then forward an online alert, such as an e-mail, to the particular subscriber (without giving the copyright owner any information identifying the subscriber); 3) the subscriber receives the alert, which ranges in severity from an educational warning to a notice that mitigation measures will be imposed on the subscriber's services.

Mitigation measures include temporary reductions of Internet speed, redirection to a landing page until the subscriber contacts the ISP to discuss the infringing activities, or other measures that the ISP deems appropriate. Although the stated purpose of mitigation measures is to educate subscribers about how to avoid infringing activities, the severity of the response by the ISP will increase for each infringing activity.

IMPACT ON PUBLIC WIFI PROVIDERS

While this system appears to provide ample warning and education to subscribers before they face mitigation measures, a business that provides free public WiFi could feasibly receive multiple alert notices for infringing activity in a single day. This puts the public WiFi provider at risk of the ISP slowing down their Internet connectivity, which could have a serious, detrimental impact. At this point, it is unclear how ISPs will penalize public WiFi providers.

Further, we have had several clients offering free public WiFi receive notices direct from copyright owners alleging that infringing material has been transmitted over the client's network. In each case, the potential of liability for copyright infringement has been raised.

In light of the above, it is our recommendation that providers of public WiFi consider taking the following measures.

DMCA SAFE HARBOR AND BEST PRACTICE

The Digital Millennium Copyright Act of 1998 ("DMCA") provides four safe harbor provisions that provide immunity to service providers (like public WiFi providers) for infringing activities that take place on their networks provided that the service providers meet specific requirements. There are three basic requirements which must be met to be eligible for any of the safe harbor provisions. A service provider must:

1. Adopt and implement a policy for terminating the accounts or subscriptions of repeat infringers (such a policy includes notifying the individual who conducted the infringing activity and ultimately blocking the individual from accessing the network if the infringing activity persists; additionally, documentation of all steps taken by the provider to stop infringing activities is necessary);

2. Inform users of this policy; and

3. Accommodate and not interfere with the "standard technical measures" that copyright owners use to identify copyright infringement and protect their copyrighted works.

Two of the four safe harbors in the DMCA are most applicable to public WiFi providers. The first safe harbor applies to service providers that only offer an Internet connection. The service provider in this case merely acts as a data conduit. For a provider to be eligible for this safe harbor, it must not interact with the content of the data transmission in any way, aside from performing the function of transmitting the data. This may apply to some public WiFi providers.

The second safe harbor provision, sometimes referred to as 512(c), applies to any provider of network access. This definition includes most public WiFi providers. For a service provider to be eligible for this safe harbor and not liable for any infringing material that resides on the provider's network by the direction of a user, the provider must have a designated agent registered with the United States Copyright Office. The designated agent shall receive and process all DMCA takedown notices of infringement. An outline of the registration process and copy of the required form can be found at: http://www.copyright.gov/onlinesp/.

Additionally, under 512(c), the provider must not have knowledge of the infringing activity, be aware of circumstances where infringement is apparent, or receive a financial benefit from any infringing activity. While 512(c) places additional prerequisites on the provider with the registration of a designated agent, it is a best practice for any public WiFi provider to comply with this requirement. Compliance with the prerequisites of 512(c) gives the public WiFi provider safe harbor protection, further shielding its business from infringing acts that take place on its network.

With public WiFi providers open to multiple avenues of potential liability, it is recommended that they comply with the requirements of the safe harbor provisions under the DMCA to shield themselves from potential liability for copyright infringement that occurs on their networks.

[1] The RIAA stopped publicly publishing the number of lawsuits it issued against individual infringers after February 2006.

James E. O'Connor is a partner with Baird Holm LLP in Omaha, Nebraska. His practice focuses on technology and intellectual property with special emphasis on cyber issues; the development, acquisition, and use of technology; and privacy and security matters. He represents clients in the financial, health, technology and cyber industries. Mr. O'Connor would like to thank AriAnna Goldstein, summer associate at Baird Holm, for her assistance with this article.