White Paper: Authenticated Access Decreases Service Abuse, Eases Burden for New Government Compliance, and Reduces Liability

December 5, 2007 5:47 PM PST

House vote on illegal images sweeps in Wi-Fi, Web sites

Posted by Declan McCullagh

http://www.news.com/8301-13578_3-9829759-38.html?tag=nefd.top

Summary
Increasing legislative interest in monitoring and enforcing anti-pornography laws over the Internet places an increased burden on operators of WiFi hotspots, including "individuals, coffee shops, libraries, hotels, and even some government agencies." In this example, legislators are requiring WiFi venues to report child pornographic activity on their network and turn over relevant information to the authorities. Failure to comply with reporting requirements results in a $150,000 fine for the first occurrence and $300,000 for subsequent occurrences. As a result, venues desiring to offer WiFi to the public must learn to manage the risks at their own expense.

Anonymous WiFi and the Open Access Point
Today, the anonymous open access point is the prevalent method for providing free WiFi to the public. This is accomplished by using an inexpensive, widely available, off-the-shelf wireless access point or wireless router and connecting it to a broadband connection. While attractive in terms of initial costs and ease of use, it becomes less attractive as a business solution when considering the entire value proposition, such as security risks to the venue, customer liability, and more recently, complying with legislation requiring the reporting of illegal activity and the retention of evidence. It is reasonable to believe that legislative interest in national security and domestic crime investigation will continue to add to the burden of providing internet access to the public.

Germany has already passed national legislation prohibiting commercially-available open access points.

The Business Risks of Providing Anonymous, Open Access WiFi

- Security Risk to Business – When improperly deployed, a venue could inadvertently allow its customers unauthorized access its business office computers containing trade secret, private customer account information, employee records, and financial information. This is a common misconfiguration of a shared network that still prevails in most small businesses today.

- Security Risk to Customer Computers – When venue customers use a wireless network, they may inadvertently share their computers and files with each other. This is a networking feature of Windows and Macintosh operating systems. It can lead to a breach of privacy, corporate espionage, theft of data, and damage to computer files.

- Security Risk from Network Abusers – People who wish to conduct illicit activity over the Internet are drawn to anonymous open access points because it is difficult to trace their activities back to them. Instead, their activities are traced back to the venue which must then respond to inquiries from ISPs, police, copyright and trademark holders, and other authorities. Too many complaints about activities occurring at a particular venue may result in Internet service termination and other consequences. At the minimum, responding to inquiries, complaints, and litigation is distracting for a business.

Commercial-grade Free WiFi

Less Networks® provides a commercial-grade free WiFi solution that enables venues to remain competitive with free WiFi but provide it in a responsible and professional manner that improves the user experience while mitigating the risks and hassles of security and legal compliance for the business.

- Mitigating the Risk to the Business – The Less Networks Smart AP™ self-installation package makes it difficult for a venue to inadvertently share its business computers with its customers. For greater peace of mind, Less Networks offers professional installation and support options to make sure that the WiFi network is deployed as safely as possible within a venue's budget constraints. Moreover, the built-in Terms of Use specifically prohibits users from gaining unauthorized access to the venue's computers and systems. In some jurisdictions, it is difficult to prosecute a "computer trespass" without a posted sign warning users against the activity. Less Networks requires that every user acknowledge the Terms of Use. These Terms of Use not only discourage unauthorized intrusion, they become instrumental in recovering damages from users who intrude into your business systems.

- Mitigating the Risk to Customer Computers – In order to prevent unauthorized file sharing, users must properly configure their computers to disable sharing. It is also recommended that they install and properly configure personal firewalls to protect themselves against intrusion from users at the venue and over the Internet. Users may also expose themselves to "electronic eavesdropping" by transmitting sensitive or confidential information over the WiFi connection.

  Unfortunately, when users suffer damages caused by their own ignorance about WiFi security, they sometimes seek to recover those damages from venues. The plaintiff attorneys will claim that the venue was negligent in informing their clients of the risks of using WiFi within their place of business. Most venues settle out of court rather than incur legal expenses and the risk of losing the suit.

  Similar to a "Caution! Wet Floor" sign, Less Networks presents all WiFi users with a "Caution! WiFi is Risky" sign in the form of a Security Statement. A wet floor sign does not eliminate liability resulting from a fall, but it does prevent falls by drawing attention to the risk. The Less Networks Security Statement draws attention to the risks of WiFi usage and then requires them to acknowledge these risks before proceeding.

- Mitigating the Risk of Network Abuse – In order to discourage prohibited activities and put users on notice, some venues have deployed "Click to Accept" Terms of Use solutions on their anonymous WiFi systems. This acceptance is insufficient because it does not explicitly tie acceptance to a particular user. It is too easy for an anonymous user to deny clicking, claim that they clicked by accident, or that the "Click to Accept" was not sufficient enough of a mechanism to warn or advise them. Without a record that links acceptance to an identifiable user account at a specific point in time, it is difficult for a venue to protect itself.

  Less Networks requires all WiFi users to create a personal WiFi account that is validated using a confirmed email address provided by the user. During the creation of this account, the user must accept and understand the Terms of Use and the Security Statement. This multi-step process makes it difficult for users to claim that they were not sufficiently advised of prohibited activities or warned about the risks of using WiFi. The account creation process itself takes less than two minutes and the account can be used again by the user at any Less Networks hotspot.

Conclusion

Although the burden placed on venues for providing free WiFi will likely continue to increase, there are solutions in the market that will help venues manage the risks associated with providing WiFi while continuing to enjoy the benefits.

Less Networks provides the most cost-effective commercial-grade free WiFi solution that can help a venue get the most business value out of its free WiFi investment while responsibly providing public Internet access.

About Less Networks

Less Networks® provides innovative sales and marketing WiFi solutions for public-facing businesses and organizations. Its flagship product, CustomerConnect™, enables venues with free WiFi to transform anonymous wireless internet service into a revenue-driving communications channel that allows a venue's customers to connect to the Internet and a venue to connect with its customers—even after they leave. It's the solution that powers the renowned Austin Wireless City Project and propelled that organization to the forefront of public wireless initiatives.

Its consumer product, Less Networks™ < Free WiFi, sets the standard for commercial-grade, high-quality free WiFi service. Available in 61 cities around the world, Less Networks™ < Free WiFi hotspots connect mobile users to the Internet over 25,000 times each month. Major brands that offer Less Networks™ < Free WiFi in their venues include Baja Fresh®, Burger King®, Dairy Queen®, Days Inn®, and Sleep Inn®.

Founded in 2003, Less Networks is headquartered in Austin, Texas.

Contact

Less Networks, LLC
sales @ lessnetworks.com
www.lessnetworks.com

+1 800 929 8891 *Toll-Free US*
+1 408 834 7703 *US Direct*
+44 207 043 9229 *UK Direct*