International

CRi

Issue 2
15 April 2006
P. 33–64

A Journal of Information Law and Technology

With Index 2004/2005

Articles

Case Law

Updates

Verlag Dr. Otto Schmidt

CRi

Articles

Benjamin D. Kern

Roaming in the USA

Using Open Wi-Fi Connections under US Law

Wireless technologies have dramatically increased the accessibility of the Internet. Because it is fast, cheap, and easy to install and use, Wi-Fi wireless LAN technology has played a leading role in this expansion. Wi-Fi has revolutionized the way people use the Internet in their homes, offices, and increasingly, in public places.

Wi-Fi access points can easily be secured by activating standard encryption technology. However, many home and office users choose not to activate this encryption, sometimes because they choose to provide Internet access to outsiders, sometimes because they are not willing to go to the trouble of securing their networks, and sometimes because they do not understand the risks of leaving a network open. As a result, open networks are ubiquitous. It is possible in almost any populated area (and many rural areas) to find an open Wi-Fi access point, and to use that access point as a means to get high-speed Internet access. In fact, the popular Windows XP operating system frequently alerts users that wireless networks are nearby, and prompts users as to whether they would like to connect, or may connect automatically, depending on the user's settings.

Using a random open network is certainly convenient. Is this practice illegal? Maybe. Should the law allow this type of access? Definitely. This article explores the legality of accessing the Internet through open Wi-Fi connections in situations where the user has not obtained prior permission from the network operator. This article will first discuss the policy considerations behind permitting or prohibiting such roaming Wi-Fi access. The article will then summarize US law that applies to this type of behavior. Finally, the article will propose an approach that legislators and courts worldwide should take to conform the law to the policy considerations identified in the article.

I. Should the Law Allow Use of Open Wi-Fi Connections to Access the Internet?

Ubiquitous Wi-Fi Internet access is an important component in the continued development and expansion of the exchange of information enabled by the Internet. Wi-Fi access to the Internet is available in many locations commercially, for a per-use fee or on a subscription basis. Commercial Wi-Fi access can be important for business travelers and others who need quality connections, security, value-added services, support or uniformity in access procedures. However, the pricing for one-time access is typically high, and the coverage of most subscription-based Wi-Fi access services is generally fragmented or limited to high-visibility areas such as airports, hotels and coffee shops. In order to fully take advantage of the Internet, connections must be available wherever and whenever users need or desire connections. While business travelers are the classic example of users who need access to the Internet from unfamiliar areas, almost any laptop owner will at one time or another find situations where roaming access can be useful. For example, many users have probably also experienced home broadband outages, or visits to the homes of friends or relatives who don't have broadband access. In a great number of these situations, particularly when negotiating the terms of using a Wi-Fi network would be impractical, or would not be cost-effective, the ability to use a neighboring home or business connection can be invaluable.

Additionally, other new networking technologies, such as mesh networking and the use of ad hoc networks between individual computing devices facilitated by wireless technologies, promise to continue the expansion of information accessibility by allowing computing devices to instantly establish communications with a minimum of formality and overhead. It is important to recognize that resolution of the controversy surrounding opportunistic Wi-Fi use, from both technological and legal perspectives, could impact the growth of future technologies.

The law should allow Wi-Fi users to access the Internet through open Wi-Fi connections, even if those users have not obtained prior express consent from the network operator, because the value of expansion of Internet accessibility outweighs any economic costs, security risks, and network operator liability concerns associated with this behavior.

1. Economic Cost to Network Operators

The cost of roaming Wi-Fi use is typically negligible to the home or business that has connected a Wi-Fi access point to its DSL or cable modem, and is not likely to noticeably reduce the operator's available bandwidth or performance. In the event that the home or business user experiences adverse effects from sharing a Wi-Fi connection, the operator can easily enable encryption on its network or otherwise control access to its network.

2. Economic Cost to ISPs

The cost to a home or business network operator, however, focuses on only one side of the bandwidth cost equation – even if the person who operates an access point does not pay for the possible increase in usage caused by roaming Wi-Fi users, an aggregate increase in usage would result in more infrastructure costs for the

▷ Ben D. Kern, Chicago. Further information about the author on p. 64.

Internet service provider ("ISP") that supplies the DSL or cable connection to the operator. However, ISPs are able to impose terms for the usage of their services on the customers who pay for the services. A service provider can protect itself by creating terms of service that appropriately reflect its expectations regarding its customers' use of its service.

Some ISPs currently permit use of their connections to supply bandwidth to roaming Wi-Fi users, while some expressly prohibit any sharing. Regardless of the cost allocations, the amount of bandwidth consumed by roaming Wi-Fi users may prove not to represent a dramatic increase in bandwidth usage to ISPs, in the aggregate. A roaming user may use bandwidth while away from home or the office equivalent to the bandwidth he or she would have used if he or she waited until returning to the home or office. In the aggregate, use in and out of the home or office may prove to be substantially equal.

A home or business likely will not pay more for bandwidth based on roaming Wi-Fi use. An ISP, likewise, may not experience increased costs in the aggregate because of roaming Wi-Fi use. If the ISP determined that its business model did not support roaming Wi-Fi use, it could prohibit the use of open Wi-Fi access points in its end-user terms. The direct economic costs of roaming Wi-Fi usage do not, therefore, present a compelling justification for prohibiting roaming users from accessing open Wi-Fi connections.

3. Security Risks

Some have argued that roaming Wi-Fi use should be prohibited because it creates security risks. Open Wi-Fi networks can, under some circumstances, provide network access to a person who uses that access to intercept data traveling over the network, to read, copy, delete, or modify files in shared directories on the network, or to engage in other destructive behavior. In one recent case, several men pled guilty to violations of US Federal and state law after accessing credit card information stored in the computer systems of the large Lowe's hardware store chain by accessing a store's open Wi-Fi network from the parking lot of the store.[1]

Because the defendants in the Lowe's case caused damage via an open Wi-Fi network, it may seem that an adequate solution is to restrict roaming Wi-Fi access. However, laws prohibiting roaming Wi-Fi access could actually undermine network security on a large scale. The theft of credit card information alleged in this case is adequately addressed by laws that target this theft, not laws that target Wi-Fi access to the Internet. Laws that purport to protect networks may give network operators a false sense of security. A network operator who relies on the law to protect his or her network against unwanted access may not take reasonable or appropriate technical measures to secure the network.

The New York legislature determined that the best approach to encouraging network security was to impose a certain level of responsibility on network operators. New York's statute prohibiting unauthorized computer use provides protection only if the computer or network operator has implemented security measures.[2] This requirement was included in the statute "'in order to encourage greater self-protection on the part of the computer industry.'"[3] As a New York court considering this provision summarized, "The legislative history of the statute makes clear that this requirement was included on the ground that '[s]uch protective devices provide the first line of defense against unauthorized intrusion into a computer system.'"[4] Several areas of law, in addition to New York's unauthorized computer use statute, promote responsible security practices by providing protection only when a user has taken security measures. The Fourth Amendment to the US Constitution protects against unreasonable search and seizure, but "in many contexts requires" that a user have a reasonable expectation of privacy in materials in order for those materials to be protected. Another example of a statutory approach that requires a user to take steps for his or her own protection is found in the Uniform Trade Secrets Act, which provides protection only for information that "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[5]

An operator that desires to prevent roaming users from accessing the Internet through its network can easily turn on encryption, which is included with all access points, and would prevent such access, or can implement alternative methods of security that would allow access to some, but not all, of the operator's network. A law that prohibits access to open networks will be far less effective in improving security than a law that encourages a network operator to adopt security practices appropriate for protecting its sensitive data.

4. Third Party Liability

Another justification for preventing roaming Wi-Fi use is the possibility that a network operator might face liability for the unlawful acts of a third-party that accesses the Internet through the operator's network. Under US Federal law, this justification is largely without merit because Internet-related legislation has clarified that those who provide access to the Internet to third-parties are not liable for the acts of these third-parties.

Legislators have recognized that entities providing access to the Internet should not be liable for the crimes committed through such access. The types of behavior most often identified as creating potential liability are transmission of copyrighted materials, transmission or receipt of pornography, and spamming. The Digital Millennium Copyright Act ("DMCA")[6] and Communications Decency Act ("CDA")[7] both include safe harbors that clarify that ISPs are not liable for content transmitted through their services, potentially including all of the types of content referred to above. While the DMCA has certain requirements that typically will not be met by

1 See Bill of Indictment, *United States v. Salcedo et al.*, (No. 5.03cr53-MCK) (W.D.N.C. Nov. 19, 2003); Criminal Docket for Case #: 03-CR-53- ALL, available at *http://pacer.ncwd.uscourts.gov/dc/cgi-bin/pacer250.pl? puid = 01094528557* (last visited Sept. 16, 2004); Entry and Acceptance of Guilty Plea (Rule 11 Proceeding), *United States v. Salcedo*, (No. 5:03cr53-McK) (W.D.N.C. June 4, 2004); Entry and Acceptance of Guilty Plea (Rule 11 Proceeding), *United States v. Botbyl*, (No. 5:03cr51-V) (W.D.N.C. June 7, 2004).

2 See generally, N.Y. Penal Law § 156.05.

3 *People v. Angeles*, 687 N.Y.S.2d 884, 886 (N.Y. Crim. Ct. 1999) (citing *William C. Donnino*, McKinney's Consolidated Laws of New York Book 39 at 284, Practice Commentary to Penal Law Article 156 (1999)).

4 *Id.* (citing Mem. of the Att'y Gen., 1986 N.Y. Legis. Ann. 232, 233 (supporting L.1986, ch. 514).

5 Uniform Trade Secrets Act, § 1(4)(ii).

6 17 U.S.C.S. § 512.

7 47 U.S.C.S. §§ 201 et seq.

operators of open networks, pre-DMCA case law makes clear that network operators that do not have knowledge of the content passing through their networks have little danger of being liable for copyright infringement. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM")[8] clarifies that liability for spam sent by a user of an open Wi-Fi network would rest with the user, not the network operator.

Whether or not the CDA, DMCA, and CAN-SPAM Acts expressly apply to all materials that may be transmitted through an open Wi-Fi network, courts have recognized that Congressional intent to absolve service providers has been very broad.

5. The Law Should Permit Roaming Wi-Fi Use

This article has argued that the law should continue to encourage the development and expansion of the Internet and the general accessibility of the Internet from new venues that will enhance the Internet's value to users. The utility of roaming Wi-Fi to users and the value of encouraging expansion of the Internet's accessibility, even when considered in light of the economic cost of this access, security concerns, and potential liability of network operators, suggest that the law should not unreasonably restrict the use of open Wi-Fi networks or contain ambiguity that would deter users from using these networks. The next section of the article will explore the treatment of roaming Wi-Fi use under US Federal and state statutes and the common law.

II. Does the Law Allow Use of Open Wi-Fi Connections?

It is likely that a number of laws in the US could be interpreted to prohibit roaming Wi-Fi use. However, because no Federal law clearly applies, an analysis of the legality of this behavior needs to include an examination of the relevant laws in each US state, most of which have not been interpreted by courts in a way that is directly on point. US law is therefore unclear as to whether a business traveler can legally use an open Wi-Fi network in the US.

This section will summarize US Federal laws that seem potentially applicable to roaming Wi-Fi use, concluding that these laws most likely do not apply. One possible exception is the Computer Fraud and Abuse Act of 1986 ("CFAA"),[9] which could theoretically restrict roaming Wi-Fi use under certain circumstances, if access without express permission is considered "unauthorized". This section will also summarize several types of state law that could apply to roaming Wi-Fi use, concluding that the application of many state laws may also depend on whether accessing the Internet through a network without express prior permission or prohibition is "unauthorized".

1. Computer Fraud and Abuse Act

The CFAA prohibits unauthorized access to a computer or network in a number of specific situations. In order to violate the most widely applicable provisions of the CFAA, a user must intentionally access a network without authorization, and must either obtain information or cause damage and a loss aggregating $5,000. Although it is possible that the CFAA could be applied to roaming Wi-Fi use, application of the "damage and loss" portions of the statute would reward a network operator's failure to implement security measures reflecting its expectations regarding access to its network.[10]

a) Intentional Access

A roaming Wi-Fi user engages in intentional access, but likely does not intend to engage in unauthorized access. An open network typically provides no indication to a user that access is unauthorized. Given that it is easy for a roaming user to access open networks, but also easy for network operators to secure their networks, it is reasonable for a user to assume that access to an open network is not prohibited. In most cases, it is therefore unlikely that "intent requirements like those found in the CFAA would be met.

b) Unauthorized Access

Whether access to an open network is considered unauthorized under the CFAA is unclear, as courts have applied a variety of tests. One test would deem access unauthorized only if a network operator has indicated that access is prohibited, through implementation of security measures or otherwise. This test would provide the same results as the New York statute referred to above, which applies only if the network operator has implemented security measures. Other tests require a court to determine a network operator's intent as to how its network will be used. Yet another test would find unauthorized use unless use has been specifically authorized by a network operator. This final test follows the approach taken by Colorado's Computer Crime statute, which prohibits access to a network unless express consent to access has been provided.[11]

c) Damage

Bandwidth-intensive roaming use of a network could theoretically cause "damage" under the CFAA by reducing the amount of bandwidth available to the network operator. Although it is possible that roaming Wi-Fi use could prompt a network operator to incur consulting costs to enable security, and such costs could reach $5,000, this result would essentially allow a negligent operator to improve its network at a roaming user's expense. This would be an unjust result, and should be rejected by any court considering this situation.

d) CFAA Probably Does Not Apply

In summary, it is unlikely that accessing the Internet through an open connection, without more, will implicate the CFAA. Regardless of which test is used to determine "unauthorized" access, ambiguity around what is authorized makes is difficult to say that a roaming Wi-Fi user intentionally engaged in unauthorized access.

8 15 U.S.C.S. §§ 7701 et seq.
9 18 U.S.C. § 1030.
10 For a more detailed discussion of the application of the CFAA and other laws to roaming Wi-Fi use in the US, please see *Benjamin D. Kern*, Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law, 21 Santa Clara Computer & High Tech. L.J. 101, 128 (2004).
11 Colo. Rev. Stat. § 18-5.5-102(1)(a).

Finally, the damage and loss requirements under Section 1030(a)(5) would only be met under extreme circumstances. For these reasons, it is unlikely, though possible, that the CFAA will apply to roaming Wi-Fi use.

2. Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA"),[12] part of the Federal Wiretap Act, is intended to protect against the unauthorized interception of electronic communications, and to protect stored electronic communications and transactional records from unauthorized access.[13] In the context of electronic radio communications, ECPA applies only to the intentional interception of encrypted content. Users of open Wi-Fi connections, by definition, access only unencrypted radio connections.

The encryption requirement is one way that ECPA distinguishes communications that are "readily accessible to the general public", and therefore not subject to a reasonable expectation of privacy, from communications that users should expect to be treated as private. This distinction between communications subject to a reasonable expectation of privacy and communications that are not arise from limitations imposed on governmental action by the Fourth Amendment of the US Constitution, which guarantees freedom from unreasonable search and seizure. ECPA, which is intended in part to govern the actions of law enforcement officers, is not necessary to protect communications that are accessible to the public.

3. Pen Registers and Trap and Trace Devices

ECPA has a counterpart statute, Chapter 206 of Title 18,[14] that governs "pen registers" and "trap and trace devices," which are designed to intercept addressing and transactional information relating to messages, rather than content. This statute is designed to allow law enforcement to intercept this "transactional" information with a court order, which is comparatively easy for a law enforcement official to obtain, rather than requiring a full search warrant, which is more difficult to obtain. The relevant definitions of "pen register" and "trap and trace devices" are as follows:

> (3) the term *"pen register"* means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted ...
>
> (4) the term *"trap and trace device"* means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication ...[15]

While a roaming Wi-Fi user's computer may receive and use certain addressing information in order to establish and maintain a connection with a network, the statute was clearly not intended to apply to Wi-Fi communications. If the statute was read to prohibit the use of devices that captured or recorded addressing or signaling information broadcast by Wi-Fi access points, every computer with Wi-Fi access would fit this definition. Virtually all Wi-Fi-enabled laptops are equipped with software that finds, displays, and sometimes records basic network signaling and addressing information; this scanning software is included in popular operating systems including Microsoft Windows XP, as well. All Wi-Fi access points broadcast information to help users identify these access points, unless this broadcast feature has been disabled by the operator. Although not explicit in the statute, the Fourth Amendment distinction between public and private communications is useful here, as well. Reading the pen register and trap and trace statutes to require a warrant before publicly-available information is collected leads to ludicrous results.

4. State Computer Crime Statutes

Most US states have statutes that prohibit intentional, unauthorized access to, or use of, computer networks. These statutes are often similar to the CFAA, but have certain critical differences. For example, some of these statutes do not require that a user actually causes damage. Whether these statutes apply to roaming Wi-Fi use depends in many cases on whether the user intentionally engaged in unauthorized access. Unlike the CFAA, some state statutes provide express requirements as to the unauthorized element of this inquiry, as well as the intent element. Some states additionally focus on the intent of the network operator or the intent of the user in determining whether access should be prohibited.

No statutes currently directly address the issue of how roaming Wi-Fi use should be treated. However, New Hampshire's legislature did consider legislation that would have addressed this issue, in a statute that focuses on the reasonable expectations of the person accessing the network. House Bill 495,[16] which was ultimately not passed by the legislature, provided:

> The owner of a wireless computer network shall be responsible for securing such computer network. It shall be an affirmative defense to a prosecution for unauthorized access to a wireless computer network if the unauthorized access meets the following requirements: (1) The person reasonably believed that the owner of the computer or computer network, or a person empowered to license access thereto, had authorized him or her to access; or (2) The person reasonably believed that the owner of the computer or computer network, or a person empowered to license access thereto, would have authorized the person to access without payment of any consideration; or (3) The person could not have reasonably known that his or her access was unauthorized.[17]

The New Hampshire bill was introduced by Representative Richard "Stretch" Kennedy, in response to the threatened prosecution of one of Rep. Kennedy's constituents.[18] Brian Williams, a technology professional, was threatened by a municipal official with prosecution under New Hampshire's "Computer Related Offenses; Network Security" statute after inadvertently discovering that a local governmental office operated an open network, and alerting the office to the security risks pre-

12 18 U.S.C. §§ 2701-11.
13 See Rep. No. 99-541, at 1, 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.
14 18 U.S.C.S. § 2511(2)(h)(i).
15 18 U.S.C.S. § 3127(3), (4).
16 N.H. H.B. 495 (LexisNexis 2003).
17 *Id.*
18 Telephone Interview with *Brian Williams* (Mar. 12, 2004).

sented by the office's network configuration. House Bill 495 was intended to place the burden of securing a wireless network on the network owner, and to make clear that negligent or otherwise inadvertent access to a wireless network would not violate the statute. The bill was passed by the New Hampshire House of Representatives, but was abandoned without significant discussion in the Senate.

In threatening prosecution against *Mr Williams*, the municipal official alleged that *Mr Williams* reasonably should have known that access was unauthorized, given his extensive experience in the information technology industry and his familiarity with the municipality and its low level of technical competence. After an exchange of correspondence with *Mr Williams*' attorney, the municipality ultimately determined not to pursue prosecution of *Mr Williams*.

Other types of state laws may also apply to roaming use of Wi-Fi, including theft of computer services statutes, statutes prohibiting interruption or degradation of computer services, interception of communications,[19] and the tort of trespass to chattels.

5. Summary

This article has argued that the law should permit use of open Wi-Fi connections to access the Internet, but has explained that current US state and Federal law is ambiguous in most cases, and that some laws likely prohibit this behavior. The next section will suggest that legislators and courts should recognize the value of allowing roaming Wi-Fi, and should adopt an approach that would prohibit access by roaming Wi-Fi users only when a network operator has taken affirmative action to indicate that access is not authorized.

III. Permitting Roaming Use of Wi-Fi

Statutes and statutory interpretation that focus on the actions taken by a network operator to indicate that access is not authorized will lead to the most efficient treatment of roaming Wi-Fi use. This approach provides clarity to users and promotes roaming Wi-Fi use, encourages responsible security practices, and provides a bright line for enforcement of restrictions on access to Wi-Fi networks.

1. Clarifying the Law

If the network operator enables security or otherwise takes protective measures, a Wi-Fi user will be able to determine quickly that access to such network is unauthorized. Requiring this type of action by a network operator as a condition to the application of criminal law would dispel the chilling effect currently created by ambiguity as to what constitutes unauthorized usage of a Wi-Fi network. A reduction of this chilling effect would promote the use of roaming Wi-Fi, and could support an important step in the expansion of the Internet and the growth of new networking technologies.

This approach also provides clarity in the law that would encourage the adoption of appropriate security measures by network operators. Clarifying that a network is not protected from access unless access is expressly discouraged would prompt network operators to be responsible in their approach to security. Once an indication that access is prohibited has been shown, the law would protect the operator's network from undesired access.

Finally, this approach would provide advantages in enforcing laws prohibiting unauthorized access. A user who accessed a secured network or secured portions of the network would be presumed to have intentionally accessed the network without authorization. Use of the software tools necessary to defeat WEP (a common form of encryption used on Wi-Fi networks) or other security means would also assist law enforcement officials and prosecutors in proving a violation of the statute.

2. Legislative and Judicial Approaches

The New York unauthorized access to computers statute provides a model statute for legislators. This statute does not apply unless security measures have been taken. Requiring security measures as a condition to application of the statute is straightforward and provides a bright-line test for what access is prohibited.

Because it is not realistic to expect widespread amendment of statutes to implement this approach, judicial approaches to implementing this test are also important. *EF Cultural Travel BV v. Zefer Corp.*[20] provides precedent for a finding that access to a network should not be considered unauthorized absent an indication to that effect by the network operator. *CompuServe Inc. v. Cyber Promotions*[21] could be viewed as precedent for finding that a user did not have the intent required to support a finding of intentional, unauthorized access unless the user had been expressly or implicitly notified that his or her access was not authorized. While CompuServe interpreted the common law tort of trespass to chattels, *Theofel v. Farey-Jones*[22] indicates that courts may look to common law trespass cases in interpreting the CFAA and other Federal statutes.

Some state statutes have implemented an approach that looks to a user's reasonable expectations in determining whether the user intentionally accessed a network without authorization. Courts should consider the context in which roaming Wi-Fi takes place in determining whether a user reasonably knew or should have known that access was unauthorized. Open networks are easy to access, and are, in fact, commonly shared with the public. General public perception and the media's treatment of roaming Wi-Fi could support a reasonable belief that access to an open network is permissible. Conversely, public warnings about the accessibility of open networks would not support a network operator's reasonable belief that an open network is secure. Finally, a court should consider the value of roaming Wi-Fi to society and to its users, in light of the low cost of this practice to network operators, in determining whether an open network user's expectations as to permissibility of access are reasonable.

19 See Del. Code Ann. tit. 11 § 2402; Fla. Stat. Ann. § 934.03; Kan. Stat. Ann. § 22-2514; N.J. Stat. Ann. § 2A:156A-3; 18 Pa. Cons. Stat. Ann. § 5703; Tex. Penal Code Ann. § 16.02; Utah Code Ann. § 77-23a-4.

20 *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003).

21 *CompuServe Inc. v. Cyber Promotions*, Inc., 962 F. Supp. 1015, 1020-21 (S.D. Ohio 1997).

22 341 F.3d 978 (9th Cir. 2003).

IV. Conclusion

Roaming use of Wi-Fi provides a valuable direction for growth and development of the Internet. Expansion of the area from which the Internet may be accessed by increasing the footprint of nationwide Wi-Fi network accessibility has the potential to contribute greatly to the expansion of current and future networking technologies. Negative aspects of roaming Wi-Fi use, including aspects associated with the use of networks that are unintentionally shared, are minimal and easily mitigated. Because of this value and the minimal associated risk, the law should encourage the roaming use of open Wi-Fi connections to access the Internet.

Current Federal and state laws may apply to the roaming use of open Wi-Fi networks. Many statutes are unclear as to whether roaming Wi-Fi use is illegal. In a number of states, and potentially under the Federal Computer Fraud and Abuse Act, application of computer access statutes depends on whether a user intentionally accesses a Wi-Fi network without authorization. Statutory and case law defining intentional access without authorization is inconsistent and ambiguous. A lack of clarity and consistency among existing laws threatens to have a chilling effect on this important direction of future growth for the Internet.

Legislators and courts should consider that the sharing of Internet connections using Wi-Fi is a common and widespread practice. It is often difficult or impossible for a user to determine whether a connection has been shared intentionally or inadvertently. In contrast, it is typically easy for a network operator to enable basic security measures on a Wi-Fi network. The substantial benefits to society of roaming Wi-Fi use are higher than the minimal costs typically associated with obtaining Internet access through an inadvertently open network.

Don McAleese/John Cahir

A European Perspective on the Peer-to-Peer Model post-Grokster

How far is European law harmonised and what triggers a filesharing company's liability in European common law jurisdictions?

The recent decision of the US Supreme Court in MGM Studios Inc v. Grokster Limited (US Supreme Court, 27 June 2005, CRI 2005, 109–115 with remarks by Wittow) has drawn a curtain on the long-running litigation between music studios and distributors of file-sharing software. The decision has been well received by most concerned parties, as it seems to strike a reasonable balance between the interests of bona fide software innovators and music copyright owners.

In essence, the Supreme Court has affirmed with qualification its earlier ruling in the Betamax case (Sony Corporation of America v. Universal City Studios Inc 464 US 417 – a case concerning the liability of VCR manufacturers for the infringing activities of home-users), where it held that makers of devices that are "capable of commercially significant non-infringing uses" are not liable for the infringing acts of third parties who use those devices. Under the Grokster ruling this exemption from liability is lifted where it can be shown that a person distributed devices (including software) with the object of promoting their use to infringe copyright, as evidenced through clear expression or other positive acts. In such circumstances the promoter of the device will be liable for the resulting infringing acts of third parties. The Grokster ruling has introduced what has been termed a new "inducement" theory of contributory copyright infringement: distributors of devices, which have a non-infringing use, will be liable for copyright infringement if they positively promote the device on the basis of its infringing uses.

While this decision provides a welcome clarification of the position under US law with respect to the liability of file-sharing software companies, the position in Europe remains uncertain. From an industry perspective, the main difficulty in assessing the liability of individual file-sharers and file-sharing companies is the fact that at present there is not a fully harmonised and unified copyright law in Europe. The entitlements of copyright owners remain creatures of national law and accordingly must be individually enforced in each of the 25 Member States of the European Union. Over the past 15 years some degree of harmonisation of Member State copyright law has been achieved, however, significant aspects of copyright law, including the concept of infringement, remain unharmonised.

This article aims to summarise and explain the liability of file-sharers under European law (to the extent that such law is harmonised) and will focus in particular on the potential liability of file-sharing companies under the EU's two common law jurisdictions – Ireland and the UK.

I. The Extent of Harmonisation of European Copyright Law

The principal constitutional basis for EU intellectual property (including copyright) legislation is Article 95 of the EC Treaty, which permits the adoption of legislative acts for the approximation of laws which *"have as their object the establishment and functioning of the internal market."* Standing against the harmonisation objective of Article 95 is Article 295 of the EC Treaty which states that the *"Treaty shall in no way prejudice the rules in Member States governing the system of property ownership"*. Member States' copyright laws are generally seen as a system of property ownership, so arguably this Article could undercut EU legislative competence in this field.

▷ Don McAleese/John Cahir, both at Matheson Ormsby Prentice (MOP), Solicitors in Dublin, Ireland. Further information about the authors on p. 64.

About the Authors

Andrew C. Alleyne is a corporate associate in the Toronto office of Fasken Martineau. He is engaged in a broad corporate/commercial practice with a particular interest in information technology. Andrew has gained particular experience in asset and share acquisitions, reorganizations, and drafting and negotiating a wide range of agreements related to outsourcings, consulting arrangements, software licensing and maintenance and support agreements (both for licensors and licensees), and Internet and e-commerce matters.

John Beardwood is a partner at Fasken Martineau DuMoulin LLP, Toronto, engaged in a corporate/commercial practice, with an emphasis on information technology and privacy law related matters. LEXPERT has ranked John as a leading practitioner in the technology law field in Canada. John works closely with clients in preparing and negotiating various technology-related transactions (including outsourcing, joint venture and e-commerce related transactions), and frequently advises clients on privacy law and access to information matters. John is a frequent national and international speaker and author regarding various technology and privacy related issues. John is vice chair of the firm Technology and Intellectual Property Group and vice chair of the firm Privacy and Information Protection Group, a founder and ex-board member of the Canadian IT Law Association (IT.Can), co-Program Chair of the International Technology Law Association (previously, the Computer Law Association), and founder and Chair of the Canadian Bar Association Privacy and Access Law Section.

Peter Blume, LLD, Ph.D. is professor of legal informatics at the Faculty of Law, University of Copenhagen; e-mail: *Peter.Blume@jur.ku.dk*.2.

John Cahir is a Senior Lawyer in the Commercial Intellectual Property Group at MOP. John advises on all matters relating to the protection and commercialisation of intellectual property rights (IPRs). In particular, he specialises in IP due diligence reviews, strategic portfolio advice and the acquisition, divestment and licensing of IPRs. A specific focus of his practice is the development of strategies for protecting and enforcing IPRs in the digital environment, including the use of digital rights management technology. John is a member of the Licensing Executives Society (LES) and a national representative of the Association Internationale pour la Protection de la Propriété Intellectuelle (AIPPI). He holds a PhD on the topic of digital copyright from the Queen Mary Intellectual Property Institute, University of London.

Probir Roy Chowdhury is an Associate in the Technology Practice Group of J. Sagar Associates and is based in Bangalore, India. He may be contacted via phone (+91-98 45 10 59 37) or e-mail (*probir@jsalaw.com*).

Benjamin D. Kern is a Partner in the Technology & Business Department of McGuireWoods LLP. His practice focuses on technology transactions, including licensing, technology transfer, services and development agreements. He represents emerging companies, particularly with respect to financing, venture capital and mergers and acquisitions, and regularly works with wireless carriers, universities, device companies, networking companies and others in the technology marketplace.

Don McAleese is Partner and Head of the Information Technology Law Group at Matheson Ormsby Prentice ("MOP"), Solicitors in Dublin, Ireland. He specialises in all aspects of computer, communications, e-commerce, internet and telecommunications technology and has been involved in some of the largest information technology contracts and projects in Ireland. He led the MOP Team that advised the Irish Department of Public Enterprise in the drafting of the Irish Electronic Commerce legislation, the Electronic Commerce Act, 2000.

He is a member of the European Commission Legal Advisory Board on the Information Market. He was also a member of the Legal Issues Advisory Group to the Irish Information Society Commission which was established by the Irish Government. He is currently Chairman of the Legal Issues Group of the Irish Internet Association. He was a member of the Focus Group convened by the Irish Department of Public Enterprise to consider the Irish legislative proposals for electronic signatures. He was a co-founder of 2000 Aware an Irish cross industry grouping whose objective was to raise awareness of the year 2000 problem in Ireland.

Dr. Grace Nacimiento is a partner at the Düsseldorf law firm BBORS, where she practices public law with a focus on telecommunications and media law as well as EU law. Her main emphasis lies in advising telecommunications companies and investors on all regulatory issues.

Prof. Dr. Olaf Sosnitza is Professor at the Faculty of Law, Julius-Maximilians-University of Wuerzburg, Germany. He is specialized in the law of unfair competition as well as intellectual property and E-Commerce-Law. E-Mail: *Sosnitza@jura.uni-wuerzburg.de*.

Rolf H. Weber, born in Zurich (1951), studies at the Zurich University and at Harvard Law School, bar exam in 1978, Dr. iur. in 1979, since then practicing attorney, admitted as special lecturer to the Zurich University in 1986, since 1995 tenure professor for commercial and international business law at the University of Zurich with communications law, banking law, antitrust law and European law as main topics.

Chiara Garofoli, LL.M., read law at the University of Pavia (J.D. summa cum laude, 2002) and at the University of Cambridge, where she specialised in intellectual property, EC competition law and international commercial litigation, obtaining a Master's Degree in 2005. Since 2003 she has worked in the Milan office of Trevisan & Cuonzo Avvocati, a leading independent Italian law firm with strong expertise in intellectual property and information technology. Chiara is an associate in the IP Department and her area of practice includes enforcement of patents and trade marks, domain names, e-commerce and general IP and IT advice for international clients. She is a regular contributor to newsletters on intellectual property issues. Chiara can be contacted at: *cgarofoli@trevisancuonzo.com*.