

Legislation restricting Internet access

August 15 2009

Laws aimed at tackling illegal use of wireless internet connections are restricting attempts to increase broadband access, according to research published today.

Daithí Mac Síthigh, a lecturer in IT and internet law at the University of East Anglia (UEA), says current legislation may not be the most appropriate way to regulate 'wifi' sharing - where a network is used by more than one person - and needs clarifying so it does not discourage people from using wireless and hold back provision of community wifi schemes.

This could also have implications for the UK Government's commitment to ensure that every home in the UK has broadband access by 2012, as set out in its Digital Britain report in June. A range of technologies, including wireless, will be used to deliver the basic broadband.

In the study, entitled Law in the Last Mile: Sharing [Internet Access Through WiFi](#), published in the online journal *SCRIPTed*, Mr Mac Síthigh suggests that there are advantages to sharing but current legislation unnecessarily restricts the development of "what would be of benefit to society". He also suggests that it is necessary to change relevant legislation to avoid giving disproportionate protection to internet service providers (ISP).

"Digital inclusion is a government policy and rightly so. People may not have broadband in every road, particularly in rural or isolated areas, and costs of a good connection remain high, so sharing internet access is

recognised as a great way of filling in the gaps," said Mr Mac Síthigh, of Norwich Law School at UEA. "Shared internet access has potential social benefits, but it's harder to encourage people to take part if the legalities are unclear. Furthermore, local communities trying to use wireless access to extend connectivity have faced objections from established industries that this is anti-competitive or a breach of contract. If the legal environment was more favourable to sharing it would play an important part in achieving the Digital Britain aim of inclusion and social goals of increased access."

Mr Mac Síthigh studied the legal restrictions and liability issues related to sharing an internet connection through wireless access points (WAP), typically via wifi routers used in homes and public places. The scope of the research included the legal provisions in the UK as well as selected jurisdictions abroad, including the United States and Europe. Points can be 'open', so any device can connect to it, or secured. However, prior research reviewed in the article published today indicates that many WAP owners do not secure their network, whether by deliberate choice or non-action, for example accepting the default settings.

The objections to sharing relate to people using networks without permission or paying, for example to illegally download music or films or to access other information and systems. It is also alleged by some experts that allowing others to use a connection can slow down internet access and impact on download limits. Criminal offences that could apply to the illegal use of open networks include dishonest use of a communications services or unauthorised access to a computer.

Given that new devices such as the iPhone are set up not just to connect to available networks but to swap with ease between mobile and wifi networks, countless users will be using open networks on a regular basis. Because open wireless access points can be found by walking down a typical street clarification and certainty in the law is needed.

Mr Mac Síthigh said: "Many people may be technically breaking the law and would not agree that using an open network should be a criminal offence, and although it's unlikely widespread prosecutions will take place, currently many ISPs restrict your ability to share via their terms and conditions of service. If you've done something to breach these terms it may have consequences further down the line and could be used against you."

In reviewing reports of the policing of internet sharing, Mr Mac Síthigh established that convictions and arrests have been made under section 125 of the Communications Act 2003, which states that "a person who (a) dishonestly obtains an electronic communications service and (b) does so with intent to avoid payment of a charge applicable to the provision of that service, is guilty of an offence". The Computer Misuse Act 1990 also creates various offences relating to the use of computers.

Mr Mac Síthigh added that current [legislation](#) originates from older telecommunications law and is designed for more serious acts like computer hacking and major defrauding of communications companies. "Malicious hacking and phone fraud should of course continue to be crimes but if wifi sharing is to be encouraged and properly regulated this is an inappropriate use of the law. People have been convicted for using networks without stealing passwords, breaching security or engaging in other antisocial activities," he said.

Source: University of East Anglia

Citation: Legislation restricting Internet access (2009, August 15) retrieved 26 April 2024 from <https://phys.org/news/2009-08-legislation-restricting-internet-access.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.