

Response from Rodney Tillotson

There are two issues arising out of one of the services likely to be provided in this way; namely, public use of wireless LANs for Internet connection. Both concern data network security and will at first appear to be a long way from the RA's remit.

1. Privacy on wireless LANs is very poor. Sensitive details including passwords and credit card numbers are commonly broadcast in plain text and this is not widely known.
2. Use of wireless LANs cannot be traced to an individual. It is not clear who can be held responsible for any abuse.

Methods of enhancing data privacy include:

- + Engineering of the coverage area. It is possible to ensure that standard apparatus can only use the service within one or more rooms or buildings, but this is rarely done. Where the service is to be provided in a space accessible to the public, the absence of privacy is a defect irrespective of coverage.
- + Link level encryption. Again this is not widely deployed. Where it is used, a motivated person can break the relatively weak encryption after gathering traffic for a few hours.
- + Data service encryption. There are standards (IPSEC) for encrypting data network traffic but they are not widely deployed in consumer apparatus.
- + Application encryption is common (though not universal) for the transfer of credit card and other details in e-commerce, using SSL. E-mail messages can be encrypted with PGP (though very few are). All traffic on an established connection, including any wireless link segment, can be made satisfactorily private with SSH; once more, deployment is limited. The same deficiencies apply for any shared medium; but in contrast with wireless LANs, users of an Ethernet LAN are more often able to tell who else may be able to read their data in this way. Traceability is crucial. This is a policy question at a higher level; the issues are about people and business relationships, rather than technology.
- + There is a balance to be struck between complete accountability which would greatly enhance the ability of the Internet to resist damage or its use for undesirable acts, and anonymity which offers individuals some privacy both from other individuals and from corporate or government agencies.
- + Current industry practice is that use and abuse should be openly attributable to a service provider but that personal data about users remains the responsibility of their provider. Recent UK legislation (HRA, RIPA, DPA) gives conflicting signals and the resulting confusion is not conducive to good practice by Law Enforcement or other agencies, nor to good behaviour by Internet users. Present perceptions about global security increase the confusion.

+ I anticipate that each public wireless LAN service would be provided under an agreement between the proprietor of the area to be served, who might operate the wireless apparatus, and an Internet Service Provider who would connect the resulting data network to the Internet. It is highly desirable that each such agreement clearly assigns responsibility for the actions of users of the service, and that the act of providing a service which can be used by persons about whom nothing is known carries serious obligations.

+ There is no immediate prospect that any practices agreed in the UK or even in Europe will eliminate worldwide confusion or abuse of either kind. It is nevertheless valid for the UK to establish and exhibit good practice.

+ In a corporate or education environment it is possible to restrict use of a wireless network to explicitly authorised computers (normally identified by their network cards) or other devices. The same level of prior arrangement will not be practicable for facilities in airports or other public places.

This aspect of Internet use is not new; analogies might be drawn with cybercafe access to the Internet, with postal, telephone (fixed and mobile) and perhaps other services. However, permitting public wireless access without clarifying the responsibilities of Internet providers could increase the scale of the problem by an order of magnitude or more within a few months. Experience in the Internet is that potential miscreants have a keener appreciation of the flaws in a system than its legitimate users.

I am concerned that the RA may not be in a position to manage the necessary interaction with the Internet industry, normally the province of a different agency. I suggest that one or more bodies able to represent Internet Service Providers in the UK should comment on the Consultation if they have not already been invited to do so. The UK industry has at least one guide to good practice in regard to traceability. I believe that similar services are already in use in other European countries and it may be that details of experience there would also be useful.

It is possible that similar issues arise in respect of other potential services.

I am in a security-related position in the Internet industry, but I send this response to the Consultation in my individual capacity. If you need any further information about myself, or explanation of any of the points I have made, do not hesitate to ask. I can also provide this note in other electronic formats or on paper if it will help.