MODEL WIRELESS NETWORKING POLICY FOR CANADIAN COURTS

Prepared by Martin Felsky, Ph.D., J.D. for the Judges Technology Advisory Committee ("JTAC"), Canadian Judicial Council
Draft 02 – approved in principle by JTAC, 2008-02-01
Draft 03 – incorporates recommended changes arising out of the JTAC meeting of 2008-02-01
Draft 04 – rewritten 2014-01-17

This document sets out the key considerations facing a court when considering how to provision a courthouse wireless network.

Overview. Across Canada, wireless internet access has changed from novelty to necessity. In homes, universities, businesses, hotel rooms, trains, buses, coffee shops, airports and even on the street, anyone with a mobile device can surf the web, check their e-mail, update their Facebook Timeline, stream music and television, upload photos to the cloud and much more.

In court, wireless access can be beneficial for many reasons. First, many Canadian court buildings are not wired with network cable. Lawyers and other legal professionals need access to their case management systems, legal research, calendars, email, case files and evidence, most of which are now stored on office networks or remotely in the cloud. Journalists and bloggers need access to their research resources and to social media and news sites to post updates (where permitted).

Even though jurors must deliberate in the absence of Google and Wikipedia, prospective and actual jury members, witnesses, and members of the public attending court spend a lot of time waiting, and to deny them Internet access for long periods of time seems counterproductive. People need to check their email from work and family; surf the web to read the news, and otherwise keep connected as they do when they are not in court, always, of course, subject to the reasonable restrictions that must be imposed to maintain courtroom decorum. Those restrictions can be addressed in an acceptable use policy, key terms of which are set out below, in paragraph 15.

1. **Purpose and scope**. The court needs to determine whether the wireless network is made available for the express purpose of supporting legal representatives who have business with the court, or a wider audience, up to and including all visitors. It is possible, though not necessarily economical, to provision more than one wireless network; for example a secure, high-speed, subscription-based network for legal representatives, and a second, open network, available to anyone in the courthouse.
2. **How to provision.** Depending on a variety of local factors, court services has the option of provisioning the wireless network itself, or bringing in a third party with

the appropriate expertise and resources. The third party can be a commercial service (much like those wireless services used by hotels and coffee shops), or a law society or other institution interested in supporting users.[1]

3. **Cost recovery**. Although any wireless LAN obviates the need for renovations, retrofitting and wire pulling or installation, there are still costs associated with establishing and maintaining a secure wireless network, including hardware, software, Internet bandwidth and the human resources required to operate, troubleshoot, manage and support the system. For large structures such as court buildings, multiple access points and repeaters may need to be installed. Proper security features need to be installed and maintained, updated and tested. Proper staffing resources must also be assigned. The court needs to consider whether the wireless network is offered free of charge, or whether a monthly or one-time charge is to be levied. An informal survey of currently available Canadian and US court networks indicates that they are all offered free of charge.
4. **Accounts and subscriptions**. Whether the wireless network is offered on a complimentary basis or not, users can be asked to log in with a username and password (as they are, for example, at airport hotspots). This allows the court to exercise some control over access and to implement various security measures including encryption that would otherwise not be possible. If the purpose of the wireless provisioning is to support the work of legal representatives, for example, then strong security controls are required. If the court prefers not to require any login, then users should be informed of the risks associated with unprotected wireless connections.
5. **Monitoring**. Once a network of any kind is provided to users, traffic and usage need to be monitored to ensure availability, continuity and quality of service. To protect the privacy of confidential client information and potentially privileged information accessed by lawyers and other legal professionals in the courthouse, content monitoring should be avoided, activity logs should be purged on a regular basis, and account information should be protected from disclosure.
6. **Website Blocking**. Some courts apply technology on their wireless networks to filter out pornographic websites or other objectionable content. If this is done, then some mechanism for overriding those filters is necessary where a legal representative has legitimate need for access. The policy could also state that the court has no control over the content of any website or Internet service made accessible though the court's wireless network and that users access the web at their own risk.
7. **Limited services**. Court networks should provide access to the Internet and not to any other services such as file or printer sharing, unless access is limited to legal professionals and printers are connected for the purpose of facilitating a proceeding.

[1] In Manitoba, the Legal Data Resources (Manitoba) Corporation (a subsidiary of the Law Society) installed and manages a high speed secure Wi-Fi system for lawyers in good standing at the Law Courts Building on York Avenue in Winnipeg.

8. **Speed**. Some courts have deliberately limited the bandwidth of their wireless networks to discourage media streaming activities (such as watching movies or television), which are considered unsuitable for a dignified courthouse environment. However, it may be better to deal with those issues in an acceptable use policy rather than by arbitrarily limiting the performance of the network, since many legitimate uses benefit from high speed, including accessing large databases of electronic documents, photographs, videos or audio recordings that have evidentiary value.
9. **Privacy**. The policy should advise users that on any wireless network privacy can be compromised through the unlawful interception of data or lawful access by legal authorities. If a legal demand is made for any information relating to the use of the court's wireless network, the court's policy should include a protocol for notifying affected users protecting privileged communications.[2]
10. **Support**. Most courts are not in a position to provide support to end users who are having difficulty with accessing the wireless network. Most court policies expressly state that users are responsible for their own hardware, software and technical support.
11. **No warranties**. Since courts are unlikely to be in the business of offering wireless networks for a fee, there should probably be no warranty of quality, availability or service level (including speed) unless the court considers it necessary. The policy should make it clear that the service is offered as a convenience and that it can be modified or terminated at the court's discretion without notice.
12. **Broadcasting**. The wireless policy should clearly remind users of the court's policy prohibiting the broadcasting of court proceedings, clarify or reference the court's blogging or live tweeting policy, and remind users that judges have the discretion in any case to make orders respecting the use of any technology in the courtroom.
13. **Limitation of liability and indemnity**. Some court wireless policies limit the court's liability (and the liability of any third party provider or licensor) for any damages caused by use or failure of the wireless network, or any security or privacy breach, and even go so far as to indemnify the court against any wireless-related claims by users or third parties.
14. **Acceptable Use Policy (or Terms of Use Agreement)**. If public access is provided, then use of the court's wireless network should be subject to an acceptable use policy, accepted upon connecting to the network. If an account and subscription is required for legal professionals or other users, then "terms of use" should form part of the subscription agreement. In any event, anyone engaging in unacceptable use of the court's wireless network should be subject to sanctions determined by the court: most usually this would mean revocation of access privileges.

[2] See "Protocol And Subscription: Use Of Wi-Fi By Lawyers In The Court House," Law Society of Manitoba (undated), http://www.lawsociety.mb.ca/news/forms/miscellaneous/WiFi%20Subscription%20Forms.pdf.

15. **Unacceptable Use - examples**. Examples of unacceptable use of wireless networking in the courthouse include:
    a. Attempting to gain unauthorized access to the network or otherwise breach security protocols
    b. Interfering with or denying service to any other user
    c. Failing to respect intellectual property rights of others
    d. Using a false identification to log in, or sharing login access rights
    e. Engaging in unlawful or fraudulent activities
    f. Creating, downloading, viewing, storing copying or transmitting material that is indecent or offensive to the public, such as sexually explicit material, hate speech, racist or sexist material, unless such material is legitimately required for court business
    g. Sending or posting defamatory messages
    h. Harassing or bullying others online
    i. Using excessive bandwidth
    j. Distributing malicious programs (malware) or spam
    k. Interfering with court sound systems or other technology
    l. Broadcasting proceedings unless specifically permitted
    m. Any use that permits a breach of privacy including collecting or disseminating information about other users or anyone else in the court
    n. Breaching courtroom decorum or a judge's order
    o. Any use that disrupts proceedings or interferes with the administration of justice