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

August 28, 2008

1. **Overview**. Across Canada, wireless[1] internet access is changing from novelty to necessity. In homes, universities, businesses, hotel rooms, coffee shops, airports and even on the street, anyone with a laptop computer and wireless card can surf the web and check their e-mail without being tethered.
2. **For all members of the public, unlimited mobility and convenience are two of the primary advantages that are driving this change**. For professionals such as lawyers and journalists, ready access to their business resources such as research databases, calendars, client files make wireless computing an important productivity tool. Finally, one of the biggest influences on the growth of wireless networking is the huge cost saving over any comparable wired environment.
3. **In a hard-wired building, every user requires an outlet and wiring to connect to a hub and servers**. For wireless connections, multiple users share access to the servers through a single access point (which is in turn wired). For older buildings especially, wireless networking may be the only economical approach to internet access.
4. When lawyers, journalists and members of the public enter any courthouse and courtroom in Canada, should they be able to use their laptops at all, and if so, should they be permitted (if not encouraged) to use wireless internet access? What is the court's role, if any, in supporting or managing such access?
5. **Concerns.** Despite the tremendous benefits of wireless internet access for all participants in the justice system there are several legitimate concerns relating to cost, security, privacy and courtroom decorum. Other potential concerns with wireless technology include range, reliability and performance.
6. ***Cost***. 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 wireless Local Area Network ("WLAN"), including hardware, software, internet connectivity and the human resources required to operate, manage and support the system. For large structures such as court buildings, multiple access points and repeaters may need to be installed. Proper security

[1] "In networking terminology, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and/or microwaves to maintain communications." Webopedia, http://www.webopedia.com/TERM/w/wireless.html.

features need to be installed and maintained, updated and audited. Proper staffing resources must also be applied.

a. ***Options for Cost Structure***. There are different structures available to courts with respect to who bears the cost of a WLAN. (We assume that judges and court staff are using a wired network.)

i. ***The court may provide WLAN access in conjunction with an larger government wireless initiative***. In this case it is important that the judiciary participate in the establishment of policies (including acceptable use policies) as they may apply differently in courts than in other government-administered facilities. Such a government-sponsored hotspot[2] can be offered for free or for a fee.

ii. ***The court may contract with a commercial telecommunications vendor or internet service provider.*** Any user desiring to access the internet would need to log into the service and pay a fee. This system would operate quite independent of the court and its networking.

iii. ***The court could establish its own locally-managed WLAN and offer the service to users for free or for a fee.*** This would be an unusual step as most courts do not "sell" services to the public.

iv. ***The court could approach a non-***commercial entity such as a bar association to establish wireless access for its members and as a public service.

7. **Security**. Since wireless LANs use radio waves to communicate between nodes,[3] they are more vulnerable to eavesdropping than wired networks. The original privacy standard for wireless LANs was called WEP ("Wired Equivalency Privacy") and was introduced in 1999. Because of notorious weaknesses that have been identified in the WEP protocol, wireless networking generally has a reputation for being dangerously insecure.

8. The weak WEP protocol has been replaced by WPA and WPA2 ("Wi-Fi Protected Access"). It is not the only way to secure a wireless LAN, but it is the most commonly used standard. Any wireless system established today must employ and maintain the latest security protocols. WPA uses encryption and other means to ensure against unauthorized network access and is considered very secure.

9. **Blueprint**. To the extent that security is one of the main concerns about the deployment of wireless networks in the courthouse, courts and government looking at the benefits of implementation should closely follow the principles set

[2] "A specific geographic location in which an access point provides public wireless broadband network services to mobile visitors through a WLAN." Webopedia, http://webopedia.com/TERM/h/hotspot.html.
[3]" In networks, a processing location. A node can be a computer or some other device, such as a printer." Webopedia, http://webopedia.com/TERM/n/node.html.

out in the *Blueprint for the Security of Judicial Information*[4] (2d edition, 2006) ("Blueprint") or the court's own current Security Policies, whichever is stricter.

10. In the Blueprint, though Policy 9 specifically addresses wireless networking, all of the policies work together to create a computing environment that is safe, secure and consistent with the principle of judicial independence. Policy 9 states:

    "Special measures must be taken to ensure the security and privacy of all remote access connections and wireless networking."

11. One of the advantages of maintaining a wired network for judges and judicial users, while providing wireless access for lawyers and members of the public is that "judicial information" as defined in the Blueprint[5] should never be able to find its way to the publicly shared wireless network. The wireless access would be secure and *public*; while the court network is also secure but *private*.

12. If the wireless network is not to be used for judicial information, then the Blueprint would not apply to it as such. The host and users would be responsible for setting, offering and accepting their own set of security policies.

13. On the other hand, if the court sets up a wireless network (either on its own or in conjunction with a public sector or private sector provider) that is accessed by judges or judicial users, then all appropriate security measures would apply to protect the judicial information.

14. For any court considering the opportunity to provide wireless networking in the courthouse, the following draft policy is offered as a model that may be modified for each court's purposes.

15. **Segregation.** One important security factor that needs to be understood when embarking on any project to provide wireless networking in the courts, is that the wireless network provided to lawyers, journalists or members of the public must be completely segregated from the court's own wired LAN, through which judges, judicial and court staff access judicial or court information.

16. **Privacy**. At the trial of John Allan Muhammad (the Washington sniper) in 2003, newspaper reporter posted stories to a blog in real-time from the courtroom.

17. In 2004, journalists at the infamous Scott Peterson trial had access to a wireless internet connection in the courtroom and were able to send real-time reports back

---

[4] Canadian Judicial Council, http://www.cjc-ccm.gc.ca/.

[5] ""Judicial information" is information gathered, produced or used for judicial purposes, but does not include:

(a) Court Services administrative policies and procedures and information specifically gathered or produced for the purposes of managing those court policies and procedures;

(b) The chronological listing of court proceedings;

(c) Exhibits, affidavits and other written evidence filed with the Court;

(d) Documents, rulings, endorsements, orders, judgments and reasons for judgment that have been issued. "

Canadian Judicial Council, *Blueprint for the Security of Judicial Information,* Second edition, 2006 para. 25.

to the newsroom. While there was a ban on cameras in the courtroom, the audio feed was supplemented by descriptive language as events were unfolding.

18. Courtroom Process and Decorum.

    a. **Technical Issues**. All wireless devices, including laptops with wireless network cards, are constantly sending and receiving radio signals. In some cases these signals can interfere with courtroom microphones, recording systems, amplifiers and other devices.

    b. **Distraction**. Any user may be distracted by a laptop with or without internet access.

    c. **Disruption**. With or without internet access, inappropriate use of a laptop could disrupt court proceedings, for example inappropriate display of images or videos; sound playing through speakers.

19. **Minor problems**.

    a. **Range**. Due to the nature of wireless networks, it is possible that users in a courtroom might be able to access a hotspot that is not supported by the court (for example if a coffee shop is located across the street, or a municipality has decided to offer all residents wireless access in a city core.) Court policy must address the situation consistently with its intent. For example, if the court provides its own wireless access point should outside signals be blocked?

    b. **Speed**. Today most wireless access is slower than the typical wired broadband connection. Thus for situations where counsel may be accessing large document collections in remote databases at trial, the court should consider providing wired access as long as all appropriate security measures are in place.[6]

    c. **Reliability**. Depending on the technology used, potential interference and other factors, wireless access could be less reliable than a traditional wired network.

20. **Other consideration for policy scope and application**

    a. **Location.** The court should consider whether policies should be different in different areas of the courthouse – for example, a distinction should be made between public areas and private areas for counsel where access could be broad in scope; courtrooms in session, where access might be limited to counsel alone, and jury rooms, where no access would be allowed.

    b. **People.** The court should consider whether the same policy should apply to lawyers who have business with the court, journalists who are covering

[6] For example, the wired access should be directed through a service provider's internet portal and never through the court's own internal network.

trials, participants (for example witnesses, juries), spectators and the general public.

21. **Consistency with other policies.** Any "Wireless Networking Policy" would overlap with other policies and practice directions or notes in effect at different courts, and these must be considered carefully to ensure consistency. For example, elements of the wireless policy might be found in a court's security policy; acceptable use policy; or etiquette/decorum practice directions or notes.

DRAFT POLICY

1. This policy sets out guidelines for the use of wireless networking in the courthouse which are intended to protect the security of judicial information, preserve courtroom decorum and at the same time allow lawyers, journalists and members of the public to enjoy the many benefits of secure and safe mobile computing and internet access.
2. The objective of the policy is to balance the growing demand for internet access in the courthouse (and courtroom) against the requirements of security, privacy, and the effective administration of justice.
3. **Scope**. This policy applies to any potential user of any public or private wireless networking system in a courthouse, and applies to judges, judicial staff, court staff, third party vendors, lawyers, other participants in proceedings, journalists and members of the public.
4. Wireless devices are permitted in court subject to the following restrictions. Anyone engaging in unacceptable use may face sanctions including forfeiture of equipment or ejection from the courthouse.
5. Unacceptable use anywhere in the ***courthouse*** includes any use that causes a disturbance, interferes with court operations, or is offensive. For example:
    a. Attempting to gain unauthorized access to any computer or network
    b. Interfering with or denying service to any other user
    c. Using technology to engage in unlawful activities
    d. 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
    e. Introducing malicious programs into any network
    f. Interfering with court sound systems or other technology
    g. Recording proceedings in any courtroom, jury room, chambers or hearing room unless permitted by law.
    h. In the courtroom, jury room, chambers or hearing room, any use inconsistent with court business
    i. Any use that permits a breach of privacy or courtroom decorum

j. Any use that disrupts proceedings or interferes with the administration of justice

6. The court takes no responsibility for the availability, performance or security of the wireless network or of any device using the network. Troubleshooting and technical support are the sole responsibility of [name organization]. All users having difficulty with accessing the WLAN or with its performance should contact [service provider].