STOLEN moments

Christopher Thrall reports

Are you a borrower or a thief? Wireless technology is changing the face of online networking — and the ethical and legal dilemmas aren't far behind

Hands up and back away from the keyboard. You could be breaking the law.

If you've got a wireless laptop, there's every chance you've already wandered onto someone else's network and grabbed some free Internet out of thin air.

In some coffee shops, airports, even hotels, it's a perk offered to customers. But with more offices and homeowners installing high-speed, wireless fidelity (Wi-Fi) connections without securing them, the practice of "borrowing" anybody's Internet is becoming fairly common.

"Wi-Fi law is still up in the air," says Jeff Lutz, a computer engineering graduate and support specialist with Matrikon Systems in Edmonton.

"The focus seems to be on the activities taking place over the connection" — by which he means illegal activities like stealing financial information, transferring files or downloading child porn — "rather than on the connection itself."

But for many surfers, the tide is turning.

In 2003, Toronto police pulled over a vehicle driving the wrong way down a one-way street and found the driver naked from the waist down and his laptop displaying a girl engaged in a sex act with an adult male. Among the charges Walter Nowakoski faced was theft of communications: he had used a nearby home's wireless hub to gain access to the Internet.

Next month, a Florida man goes to court, the first U.S. person to be charged with unauthorized access to a computer or network. He was caught in his parked SUV working on his laptop outside his "victim's" house.

According to local computer guru Brad "RenderMan" Haines, using computing resources or networks of someone else without permission fits under the "theft of services" statutes and is stealing, plain and simple. Under Section 9 of Canada's Radio-Television and Telecommunications Commission Act, it's not illegal to go looking for these networks, but broadcasting on them is against the law.

It's that thin line that separates the network security consultant's legal hobby from criminal charges: as a "wardriver," RenderMan drives around with a laptop and a directional antenna in search of Wi-Fi networks.

And his findings are fascinating. Out of nearly 20,000 access points detected in metro Edmonton, 28 per cent were completely unprotected.

All wireless Internet hubs come with a number of security features, but experts say most are installed without initiating these features — despite the fact that default settings are easily found online.

RenderMan publishes the results of his Wi-Fi detection efforts on his website, www.renderlab.net. He presents the information as a public service and advises unprotected network owners to learn how to protect themselves, but absolves himself of any moral responsibility for the information.

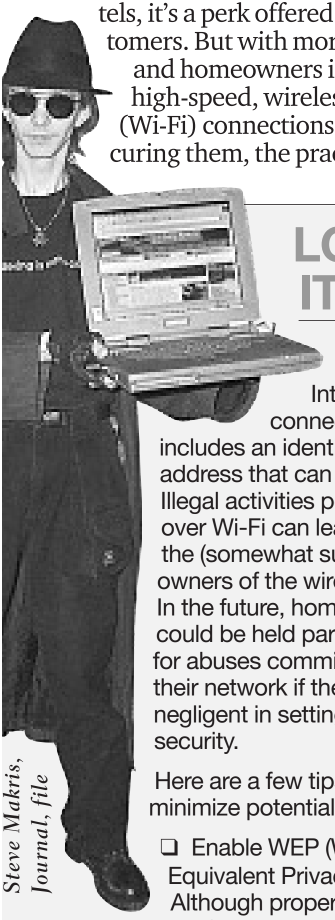
A less ethical person, of course, could use the detailed maps to enjoy free, anonymous Internet access at any time.

But before you race out with your laptop, there are three big risks to indulging in a free Wi-Fi connection. First … it's illegal, remember? The second risk is "sniffers" and the third is "rogue access points."

Sniffers monitor nearby radio transmissions and extract information from them, which is actually completely legal, according to RenderMan. Rogue access points (or "evil twins") mimic a legitimate Wi-Fi gateway. Rogues pass the user's information to a real access point, skimming anything it wants as it relays information back and forth. Both sniffers and rogues can be run from a cheaply refurbished laptop at the next table.

"Setting up a sniffer program for Wi-Fi is easy to do with free software," says Lutz. "Less and less skill is required. Setting up an evil twin, however, requires knowing the system they are trying to mimic."

See WI-FI / Page 4



Steve Makris, Journal, file

LOCK IT UP

Every Internet connection includes an identifying address that can be traced. Illegal activities performed over Wi-Fi can lead back to the (somewhat surprised) owners of the wireless hub. In the future, homeowners could be held partially liable for abuses committed over their network if they are negligent in setting up their security.

Here are a few tips to minimize potential threats:

❑ Enable WEP (Wired Equivalent Privacy). Although properly set up WPA (Wi-Fi Protected Access) is more secure, even weak encryption is better than none.

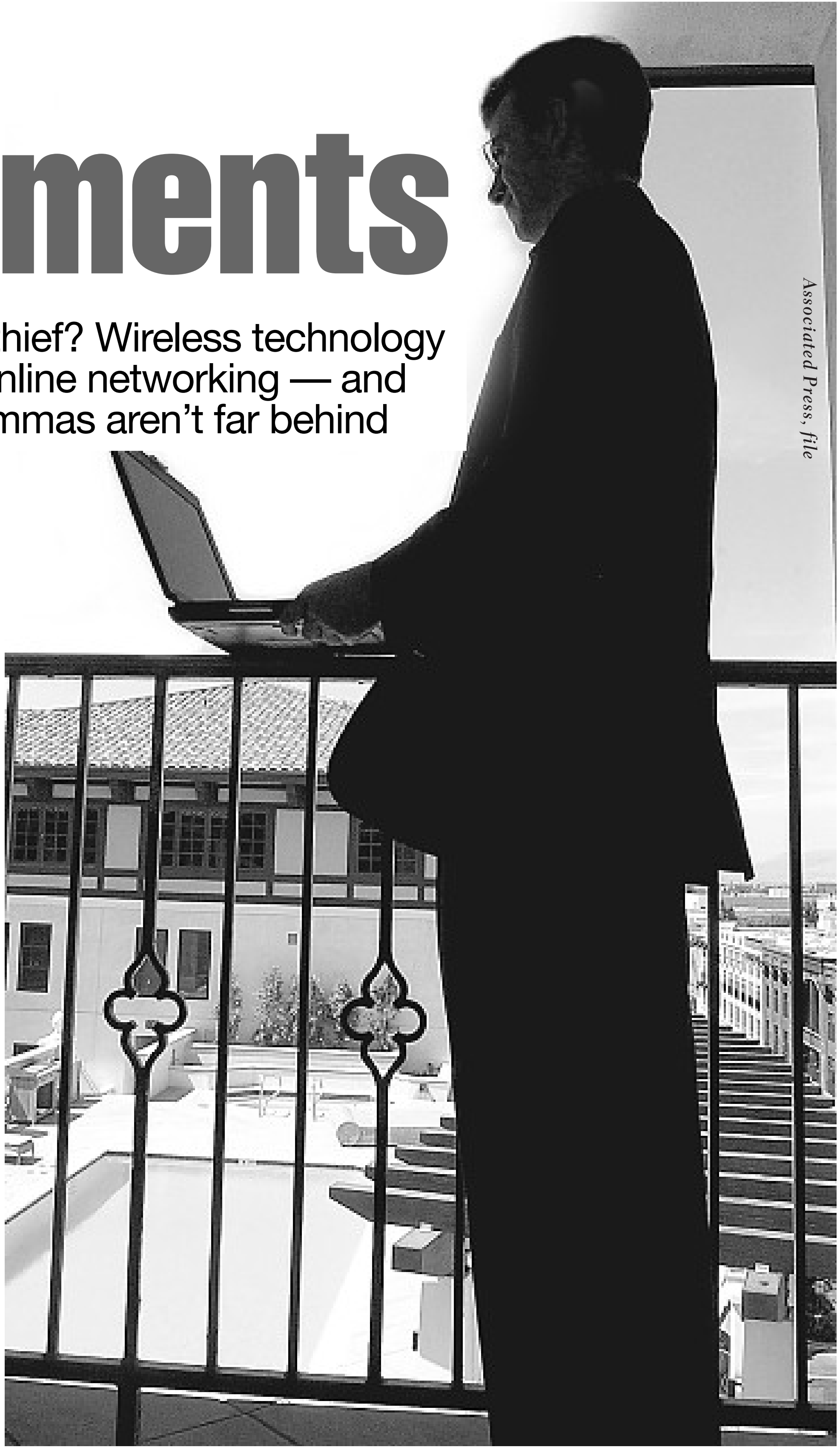
❑ Position your access points toward the centre of the building to minimize signal leak.

❑ Change your SSID (Service Set Identifier) to something nondescript. Avoid using the default setting or posting your name and address for any stumbler to see.

❑ Change the default password on access points and consider enabling MAC (Media Access Control)-based filtering to give access only to your own wireless devices.

❑ Don't send sensitive files or initiate secure transactions over Wi-Fi.

❑ Finally, turn off access points when not in use to avoid having them mapped by wardrivers in the middle of the night.



Associated Press, file

Is there a more awkward place to use of Wi-Fi technology? At left, it's RenderMan!