THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
May 2006 • Volume 6 • Number 5
Editor: Kirk J. Nahra

Handheld Online "Helper" Applications: Convenience, But at What Cost to Privacy?

Professor Jonathan I. Ezor

Jonathan I. Ezor

The Internet always has been a collaborative medium, with volunteers developing and maintaining the technological underpinnings of the global computer network, even as commercial users utilize it for a profit. Recently, though, a number of different types of services have emerged which purport to assist users in accessing the Internet in different ways and from different devices, often for free. While the majority of these services are legitimate, they pose serious potential privacy concerns that must be examined before using or recommending them.

Handheld Devices and Helper Applications: History and Today

Perhaps the most potentially troublesome and apparently innocuous are the intermediaries or helper applications. These products allow users of handheld devices (such as Palm or PocketPC handhelds, hiptops like the Blackberry, and smartphones like the Treo 650) with Internet connectivity to access popular Web sites and Internet services. The appeal of these products is clear. Handheld users often face dual challenges when trying to access Web sites and resources. First, sites may be designed for full-sized monitors and may require advanced software such as Java or Flash, or multiple browser windows to fully use them, while the handhelds have smaller screens and less-capable browser programs. Second, handheld devices often are limited in the amount of bandwidth they have to connect to

See Handheld Helper Applications, page 3

Local Security Laws: First-of-its-Kind Westchester County Proposal Would Regulate All Commercial Use of Wi-Fi

California Looks to Regulate Disclosures Relating to Use

Mary Ellen Callahan, Yaron Dori and Jamillia Ferris

In a novel attempt to enact consumer privacy laws at the local and state levels, two legislative proposals to regulate Wi-Fi and its disclosures relating to its use are now pending. The first is a first-of-its-kind proposal in Westchester County, New York, to regulate the commercial use of all Wi-Fi networks — including those used by public Internet access sites, or "hot spots," and commercial businesses — in an effort to safeguard consumer data. The second is a California bill that would require makers of wireless devices to warn consumers about the danger of unauthorized users tapping into consumers' wireless connections. The Westchester County proposal represents the first time a local government has attempted to enact regulations intended to protect consumer privacy, an area ordinarily left to state and federal regulation.

See Local Security Laws, page 5

This Month

ment used to be limited to hobbyists, today it is both big business and potentially big trouble. The end result is that, just as desktop computer users need to be careful what software they install, and how it interacts with their systems (i.e. spyware and other malware), connected handheld device owners must exercise similar discretion. On the organizational level, IT administrators and privacy professionals must educate their colleagues about the potential risks raised by "cool" applications for PDAs, smartphones and hiptops, and establish both policies and technical limitations to limit the exposure faced by the organization. If a user wants to install a particular application, he or she will have to do some due diligence to determine who is actually behind the application, to what information it has access and whether it reduces the security of the communication it is "facilitating."

Jonathan I. Ezor is the Director of the Touro Law Center Institute for Business, Law and Technology, and an Assistant Professor of Law and Technology. He also serves as special counsel to The Lustigman Firm, a marketing and advertising law firm based in Manhattan. He also is currently acting as the Reporter for the New York State Bar Association E-Filing Taskforce. A technology attorney for more than a decade, Professor Ezor has represented advertising agencies, software developers, banks, retailers and Internet service providers as well as traditional firms, and has been in-house counsel to an online retailer, an Internet-based document printing firm and a multinational Web and software development company. He is the author of Clicking Through: A Survival Guide for Bringing Your Company Online (Bloomberg Press, 2000) (www.clickingthrough.com) and coauthor of Producing Web Hits (IDG Books, 1997). He may reached by email at jezor@tourolaw.edu.

Local Security Laws

continued from page 1

Westchester County Legislation

The proposal — which was introduced by Westchester County Executive Andrew J. Spano and is referred to as the "Public Internet Protection Act" — would, if enacted, require businesses in Westchester County to develop and implement higher safeguards than in other locations in connection with their use of Wi-Fi networks. The proposal is part of an ominous trend in legislative and regulatory activity (at local, state and federal levels) intended to address "online security" without adequately considering the ramifications, including costs, on businesses that use and rely on technology. This disturbing development was recently highlighted in California where the General Assembly is considering legislation that would require makers of wireless devices to warn consumers about the danger of unauthorized users tapping into consumers' wireless connections. Equally troubling is that the Westchester County proposal — and others like it at all levels of government — could impose restrictions on businesses that use Wi-Fi networks without providing clear guidance to assist with compliance.

When introducing the proposal late last year, County Executive Spano argued that, as Wi-Fi becomes more prevalent, the threat that personal information will be exposed increases exponentially. In his view, government-mandated precautions therefore are necessary to protect that personal information, and, more generally,

> *"... In the wake of ongoing consumer data breaches, local governments are becoming as eager as state and federal authorities to enact laws and regulations to safeguard such data."*

consumers in Westchester County. To demonstrate this point, Westchester County's Chief Information Officer, Norman Jacknis, toured downtown White Plains with a laptop and wireless modem and identified 248 wireless "hot spots" — that is, areas in which a wireless Internet connectivity signal was available — in less than half an hour. Apparently, more than 120 of those hot spots allegedly lacked any perceptible security features. It was reported that some hot spots also had not changed the network's default identifier to a unique identifier (although for some public access Wi-Fi hot spots, retaining certain "default" settings may be appropriate to permit multiple people to access the network).

Spano used this information as the basis for his proposal. The proposal's stated purpose is to prevent unauthorized access to consumer data, particularly where Wi-Fi networks are involved, although the language of the proposal suggests that its scope could apply more broadly. Specifically, the proposal would require every commercial entity that offers "public Internet access" or that "stores, utilizes or otherwise maintains private information electronically" — including Social Security numbers, driver's license numbers or credit card information — to secure and prevent unauthorized access to all such information.

While it appears that the term "public Internet access" is intended to mean only Wi-Fi network access, the term is defined more broadly in the proposal. Therefore, it appears that all commercial businesses that provide public Internet access or maintain consumers' private information electronically, and use Wi-Fi networks for internal purposes, would be affected.

In addition to safeguarding consumer data, the proposal would require commercial entities providing public Internet access to conspicuously post a sign stating that the use of such access by consumers may place their personal information at risk. Additionally, all affected entities would have to file a notice of compliance with Westchester County.

*See **Local Security Laws**, page 6*

Local Security Laws

continued from page 5

The proposal's introduction clearly is most important to companies that have a presence — or support franchisees, partners or affiliates with a presence — in Westchester County, particularly those that rely on Wi-Fi technology for their own internal operations or provide wireless hot spots to consumers. For companies large and small that rely on or operate Wi-Fi networks in Westchester County, the costs of doing business in that county would increase — in some cases significantly — as a result of this proposal. But even companies that do not use Wi-Fi networks, or which are located outside of Westchester County, could experience an increase in costs if they do business with entities subject to the proposal that pass on their cost increases to customers. In the end, businesses either will have to absorb these new costs, or, more likely, build them into the prices they charge consumers for their goods and services. A spokesperson for Spano downplayed the cost to businesses, stating that their position is that "the costs would be minimal if anything," referring to the availability of free software that businesses could download to provide this protection.

It is not clear that the proposal, as drafted, would provide any significant additional protections to consumers or businesses, as the proposal's implementation process and standard for compliance with the act's "secure and prevent unauthorized access" provisions have not yet been determined.

The proposal is slated for consideration and possible enactment later this year. Violators of the new law would receive a warning for the first violation, a $250 fine for the second violation and $500 for each successive violation.

The Westchester proposal may signal the beginning of a new trend toward the enactment of consumer privacy laws at the local level, which could make compliance across large geographic regions costly and burdensome. The Westchester proposal is apparently the first of its kind among local governments in the U.S., and suggests that, in the wake of ongoing consumer data breaches, local governments are becoming as eager as state and federal authorities to enact laws and regulations to safeguard such data.

California Legislation

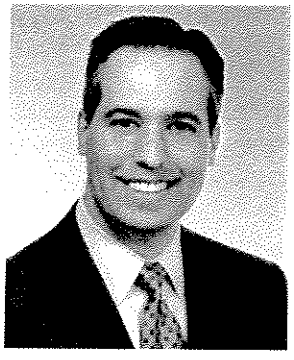
As noted above, California also has entered the debate over Wi-Fi security by offering its own legislation to address concerns over unauthorized access to wireless connections. The California legislature is taking a different approach than Westchester County by proposing legislation that would place the burden on the makers of computer network devices to warn consumers about how to protect their personal information while using Wi-Fi devices.

Assembly Bill 2415, as amended, which just cleared the Assembly Utilities and Commerce Committee on May 9, would impose warning requirements on manufacturers of "wireless network routers, wireless network switches, or a wireless network bridge" that are sold in California "for use in a small office, home office, or residential setting." For all products sold as of July 1, 2008, these manufacturers would be required to warn consumers of potential unauthorized access in one of three ways by: (1) Applying a temporary warning sticker over the ports of the device that would prevent the user from using those ports until the sticker is removed; (2) Including a disclosure in the configuration process for installing the device; or (3) Providing other protective measures that require action on the part of the consumer before the device could be used. The warning also must advise consumers how to protect their personal information. While this approach is more limited and better defined than the Westchester County proposal, it places the onus for protecting against unlawful activities on the business community. Furthermore, this development, coupled with the Westchester County proposal, suggests the clear possibility of the worst-case-regulation scenario emerging, in which some businesses are forced to comply with regulations at three different levels — federal, state and local — for a single activity.

Conclusion

As with the rash of state data breach notification laws that were enacted in 2005 (28 states as of the date of publication) following highly publicized data breaches, if the Westchester County proposal or the California legislation are adopted, there is a strong likelihood that the proposals — regardless of their current deficiencies — will be copied and introduced verbatim, or with only minor adjustments, in other local and state governments around the country. To the extent similar local and state laws and regulations are enacted as a result, it will become very difficult and costly for businesses to comply across broad regions, given the patchwork of regulations that will emerge.

Mary Ellen Callahan



Yaron Dori

Jamillia Ferris

Mary Ellen Callahan (CIPP) and Yaron Dori are partners at Hogan & Hartson L.L.P. Their practice focuses on privacy, telecommunications and data security issues. Jamillia Ferris is an associate who works with them on such topics. They may be reached at mecallahan@hhlaw.com; ydori@hhlaw.com; and jferris@hhlaw.com.