

# Mobile commerce developments worry privacy commissioner

In her 2000 Annual Report, Ontario's Information and Privacy Commissioner Ann Cavoukian expresses concern about the threats to privacy that wireless technology can introduce. According to Cavoukian, "if not implemented with an up front commitment to privacy — through legislated protections and embedded in the design of the technology itself — wireless technology may pose significant challenges to privacy."

Of particular concern is advanced GPS and radio direction-finding technology, which is expected to be incorporated into cell phones in the near future.

Such technology will be required in order to comply with the E911 initiative that goes into effect in the United States later this year. When a person dials 911 from a cell phone in the U.S., the emergency services will be able to locate the phone to within 20 metres.

Of course, other non-emergency uses will also be possible. For example, parents may be able to track their children's whereabouts. Also, businesses may be able to send geographically targeted advertisements using SMS messages to cell phones that are nearby.

Cavoukian cautions that as helpful as these new capabilities are, we must approach them with caution, as location-tracking information — combined with a date and time stamp — can have serious privacy implications.

Based on existing internationally recognized fair information practices, the commissioner suggests privacy goals for wireless technology:

Restriction of data collection and retention. This is a fundamental principle of fair information practices and needs to form the basis of any wireless infrastructure. The amount of personal information collected via the Internet may ultimately be dwarfed by what will be collected through wireless technology. Organizations need to introduce strict controls for what is collected and introduce automated purging procedures deleting anything beyond basic information



## Bits and Bytes

By Alan Gahtan

needed for a particular transaction.

Provision of encryption. The user's point of access (cell phone or other personal digital assistant) must start the encryption process. The process needs to be end-to-end in order to be truly effective and should only take place with trusted intermediaries. The question of encryption key management — deciding who should have access to the keys that lock and unlock the data — must also be addressed. From a privacy perspective, it is critical that the encryption keys remain in the hands of consumers.

Creation of an open platform for wireless devices. Users should be able to select and activate privacy and security technology that is independent of the particular cell-phone manufacturer or carrier. Currently, there are competing platforms in North America, but none of them allow consumers any choice regarding privacy.

Use of open-source technology. All technologies that "touch" a consumer's data must be accessible to public scrutiny. The technology components that comprise the wireless infrastructure, including encryption systems, data transport mechanisms, and systems architecture, should be open to allow for objective expert analysis.

De-linking transaction data. The wireless infrastructure needs to ensure that any personally identifiable information is used only for a particular transmission. Location and time data needs to be separated from personally identifiable data.

A full copy of her report is available at [www.ipc.on.ca/english/pubpres/ann\\_reps/ar-00/ar-00e.htm](http://www.ipc.on.ca/english/pubpres/ann_reps/ar-00/ar-00e.htm) **11**

*Alan Gahtan is a partner with Mann & Gahtan LLP and with the U.S. law firm Brown Reysman Millstein Felder & Steiner LLP where he practises information technology and e-commerce law.*