US telecoms regulator tackles mobile privacy

Report by Robert N Veeder

AS THE TELECOMS INDUSTRY moves towards the next generation of mobile networks, privacy issues surrounding location-based technologies have been raised. Robert N Veeder looks at the regulatory efforts being made by the Federal Communications Commission (FCC).

The world is in the midst of a wireless revolution that soon will usher in new technologies, products and services that will allow us to be connected all the time, anywhere, and to anyone. The revolution is here. It is now.

If you believe that, I have a hardly used satellite phone system I'd like to sell you for very little money.

While a fully fledged revolution may be a bit farther down the road, and is likely to depend on the development and deployment of wireless devices that are less user-hostile than the current crop, there are some interesting things happening. During the Second Annual Privacy and Data Security Summit, sponsored by the International Association of Privacy Officers (IAPO) and held Washington DC during February of this year, Peter M Connolly of Holland & Knight LLP, laid out some of the key issues in so-called m-commerce ("m" for mobile). He noted that an increasing percentage of the workforce is using wireless devices such as cell phones and personal digital assistant devices (PDAs) like Blackberry and Palm computers. He also cited a dramatic growth in the personal use of wireless devices, driven in part by operating systems and technologies that make it relatively easy to create wireless network connections.

Connolly pointed out two developments that may greatly expand the scope of m-commerce. First, emerging wireless technologies will greatly expand capacity for sending and receiving wireless data. This self-styled Third Generation Wireless (3G) will vastly increase the ability to access higher data speed for a variety of purposes, including full motion video and online games.

All this assumes, of course, that the FCC, which allocates the spectrum used for mobile networks, can find enough capacity for 3G. This is not a trivial concern, especially since there are many competitors lining up for this valuable bandwidth. Moreover, a significant user, the military, is now unlikely to release any of its own allocation for civilian uses, a restriction that was not expected prior to the events of September 11th.

LOCATION TECHNOLOGY

The other key driver is the development of wireless location tracking technologies that could create many new commercial opportunities. Location tracking technologies that can pinpoint a subscriber's position to within a few metres will combine with user preference data services. Think of the exciting possibility of having the McDonald's Corporation send you information showing the location of nearby fast-food restaurants as you drive by. Or being able to buy a soft drink merely by waving your mobile phone at a vending machine. Or being freed from a car wreck by a rescue unit that is able to arrive quickly at your precise location. While you wait to be rescued, you may be able to watch a full motion movie on your phone. These are exciting times!

PRIVACY JURISDICTION

It is especially these location finding services that pose new challenges to privacy. The historic role of the FCC has been to regulate the use of radio spectrum; it does not have primary responsibilities for law enforcement or for market regulation. These belong generally to the Department of Justice and the Federal Trade Commission. Nevertheless, the FCC finds itself confronted with privacy issues created by the emergence of 3G wireless. In his presentation to the IAPO, Connolly pointed to several proceedings currently before the FCC that deal with wireless privacy issues. These are enhanced 911 emergency services; customer proprietary network information (CPNI); and a petition asking for wireless privacy rules.

EMERGENCY SERVICES

In the US, "911" is generally the number a subscriber dials to reach an emergency response unit. According to the Cellular Telecommunications Industry Association (CTIA), in 1998 there were 35 million wireless 911 and distress calls, or 98 thousand calls per day.

The problem with using this service is that surveys have shown

nearly 40 per cent of wireless callers do not know where they are with enough precision to be able to direct a response unit to their aid: thus the need for enhanced 911 (E-911) that would use or develop new wireless technologies to identify the location of the wireless caller. The events of September 11th have greatly intensified demand for this feature.

The ultimate goal is the development of a nationwide communications infrastructure for emergency services. The US Congress gave this effort a push by passing the Wireless Communications and Public Safety Act of 1999 (WCPSA). Under the WCPSA, the FCC is required to draft the conditions and methods for providing E-911 services.

The FCC is implementing E-911 in two phases:

1. Mobile network operators are required to inform public safety answering points of the phone number and general area from which a call was made and the cell site or base station (phone mast) which received the call.

2. Operators are required to provide automatic location information (ALI) using either handset (incoporating global positioning system chips) or network-based technology. Indeed, carriers were supposed to begin implementing ALI by October 1st 2002. However, many have sought waivers because of the prohibitive costs involved. By the end of 2002, however, 100 per cent of all new digital handsets must be ALI capable. By December 31st 2005, 95 per cent of the subscriber base will use ALI-capable handsets.

Better targeting

In terms of accuracy, carriers must be able to locate a caller within 50 meters for 67 per cent of calls and within 150 meters for 95 per cent of calls using handset-based technologies. For network-based technologies, the ranges are greater – within 100 meters for 67 per cent of calls and within 300 meters for 95 per cent of calls.

So, the government is effectively creating a situation where it will be possible to pinpoint the location of an individual carrying a wireless device within a radius of 150 to 300 meters – whether they want to be located or not.

In addition to emergency services, this technology has a number of interesting and potentially useful benefits for consumers. But equally, there are advantages for third party data users. Marketers can target adverts based on where you are at any point in time. Employers can ensure their staff are where they should be by tracking their location; car rental companies can find out if you speed in breach of your rental agreement; law enforcement agencies can establish your presence at the scene of a crime or accident.

From a privacy perspective, however, it is the same old story; namely, who gets to use the data and for what purposes; who owns the data; how should it be protected; to what extent does the data subject have the right to know about its existence and uses, and participate in its creation and use; who enforces the rules; and what are the penalties for non-compliance?

Regulatory confusion

Under current law, carriers have to treat user location information as "customer proprietary network information" (CPNI). They may use the data only for E-911 or emergency purposes, unless the user gives express prior authorisation. While this sounds good, the FCC has had a difficult time regulating in this area. It is unclear what services and providers are covered and to what extent. It is unclear whether the States can regulate in this area or are preempted by the FCC. It is unclear what has to happen for "express prior consent" to take place.

Moreover, in 1999, the US Court of Appeals for the 10th Circuit threw out the FCC's initial attempt to regulate CPNI finding that the FCC "notice and opt-in" requirement was unconstitutional. The court held that CPNI was protected "commercial speech" for purposes of the First Amendment's free speech clause and that the FCC's approach was not narrowly tailored because the FCC failed to adequately consider a less restrictive "opt-out" solution. The FCC interpreted the Court's decision as applying only to a very narrow portion of its regulation in relation to the requirement for an opt-in mechanism. Thus, it is now back in the rulemaking/data gathering mode in attempting to weigh more broadly the opt-in/out issue.

Currently, interested parties are beginning to make their voices heard on this issue. The Cellular Telecommunications and Internet Association (CTIA) has asked the FCC to adopt location privacy rules of a fairly basic kind. They would require that customers be informed of carrier information collection practices prior to collection and be given an opportunity to consent as to how any information is used. They would also be assured of the integrity and security of any location information that is collected. The CTIA argues that these basic principles will let carriers provide enhanced services whilst safeguarding privacy. Carriers, on the other hand, argue that there is no need for additional restrictive rules.

From a privacy perspective, the attitude of carriers is not reassuring. It is, however, understandable given the lack of FCC activity in this area. Moreover, since the rollout of 3G data services seems far down the road, there may be time to address the privacy concerns.

Robert N Veeder is Director of US-based The Privacy Advocates.

For more information on the FCC's work, visit http://wireless.fcc.gov

The CTIA's website provides news, event listings and research on the wireless industry. See: www.wow-com.com