

**WIRELESS LOCATION TECHNOLOGY:
THE ULTIMATE CHALLENGE TO PRIVACY**

**Evan Hendricks
Editor/Publisher
Privacy Times
(Founding Member, US Privacy Coalition)**

**Before the
XXIII International Conference Of Data Protection Commissioners
September 24, 2001
Paris, France**

It's well known now that wireless communications, enabled by location-based technology, poses new threats to privacy. In fact, wireless communications, if implemented without vigilant attention, hits nearly all of the major privacy buttons: spam, richer profiles, tracking location. To some extent, e-commerce companies skyrocketed in valuation because of their perceived ability to spam, to acquire customers and to build rich profiles of individuals. It's only with hindsight that we see that failure to handle privacy, to assure consumers that their data would not be vulnerable or misused, and that their credit card numbers would be safe, emerged as a major barrier to successful e-commerce. Many dot.coms, better described as dot.bombs, have paid dearly for this miscalculation.

To its credit, the wireless industry in the United States recognized these mistakes and moved to show that it would not repeat the privacy miscalculations of the e-commerce industry. In the Fall of 2000, the Cellular Telecommunications & Internet Association (CTIA) became the first industry group in the United States to petition the federal government for binding, opt-in privacy rules. Specifically, the CTIA petition, which is still pending before the Federal Communications Commission, asked the FCC to adopt rules that would prohibit the collection of location information from cellular phone users unless they opted in to such collection. CTIA reasoned that given customers' privacy-related recalcitrance to participate in e-commerce, a strong privacy regime was needed to gain consumer confidence and encourage participation. The CTIA even warned that the FCC rules might not be adequate, as they only applied to "carriers," defined by federal law as traditional phone companies. The problem was that smaller, technologically savvy firms could provide location-based services beyond the FCC's jurisdiction. Subsequently, Sen. John Edwards (D-N.C.), a potential Presidential candidate in 2004, introduced legislation that would create an opt-in standard of any location-based service, whether provided by a carrier or non-carrier.

The CTIA's action was a watershed, not only because no U.S. industry previously had sought binding privacy rules, but also because it signified a turning point, in which major corporations recognized that privacy, rather than a hindrance, was an integral part of commercial success. The follow up by the FTC and Sen. Edwards added momentum, generating hopes that a stronger U.S. privacy regime was in the making.

Unfortunately, it appears that much of that political momentum has slowed to a stop -- for now at least. The momentum weakened over the summer with the weakening economy. The tragic attack on the New York World Trade Center (WTC) promises in the short-term to greatly reduce the prospects for pro-privacy actions.

Meanwhile, development and application of location-based wireless technologies continues in ways that could prove ominous for privacy. Much of this development, and the applications, are proceeding without adequate analysis of the potential impact on privacy. This is largely because the U.S. system does not require such analysis. An important aspect of any solution is to require that companies assess the impact on privacy that their technology and applications will have, much like industrial firms are required to conduct an environmental impact analysis.

Consequently, some institutional forces, both commercial or law enforcement, already are seeking to take advantage of wireless technology's location-surveillance capabilities.

U.S. Public Opinion (Pre-WTC)

The most authoritative survey of Americans' attitude toward wireless location services was conducted early in 2001 by Forrester Research, of Cambridge, Mass.

The survey of 1,503 consumers revealed that 71% said they were "not likely" to agree to receive location-based ads or offers to their cell phones, while 13% said they were likely to agree. Similarly, 70% said they would not see location-based ads as useful. While 55% said it was likely that location-based information would "fall into the wrong hands" if government had access to it, 61% said such a fate was likely if business had access. Finally, 43% said location-based ads would threaten their privacy, while 25% said it would not.

Overall, 70% said they were "extremely" or "very" interested in seeing Congress pass Internet privacy legislation; 72% said it was a major privacy violation for businesses to collect and then supply data about you to other companies. Only 6% said they trusted Web sites with their personal data. Fifty percent said they read privacy policies on Web sites.

"The location-privacy issue sparked by new wireless technologies is only the leading edge of a broad upheaval in attitudes toward the circulation of personal information. Smart companies will act now to insulate themselves from the spreading revolution by taking a whole-view approach to privacy," wrote Forrester Analyst Jay Stanley.

There is little doubt that in the near term, American public opinion about privacy could modify. The mainstream media has carried a steady drumbeat of messages from security and intelligence officials and experts that Americans must be willing to trade their individual privacy for improved public security. But intelligence officials basically are asking for greater authority to wiretap the *content* of communications, as well as greater freedom to recruit "unsavory"

informants and to engage in political assassinations. These objectives do not directly relate to the kinds of privacy issues that consumers said they wanted in the Forrester or other surveys. The current crisis also does not change the dynamic that consumers will be less willing to participate in m-commerce if their privacy is not protected.

Wireless Location Mandate & Technology

A central driver of the U.S. debate is a 1999 Wireless law requiring that cell phones transmit location (within 100 feet) to emergency 911 services by October 2001. (Many carriers say that they simply cannot meet this requirement and have asked the Federal Communications Commission for an extension of the deadline.) The 1999 law also has a privacy provision requiring that carriers obtain consumers' consent before using their location-based data for secondary purposes.

Currently, there are two ways to comply with the E-911 requirement. The first is the Global Positioning System (GPS). By placing GPS chips in handsets, GPS is able to draw on satellite technology. It is most commonly used by automobile on-board navigation and directions services and is the choice of Sprint PCS, a U.S. wireless carrier.

The second system is a "network based" approach, which relies on the strength of the cell phone's signal and triangulation between the cell towers carrying the call. Some carriers, like Verizon, are using this approach. Others, like Cingular Wireless, said it would use a hybrid between GPS and network cell tower triangulation.

Possibly the most important aspect about cellular technology is that each telephone transmits a unique identifier. This enables the cellular phone to communicate and identify itself as it passes from one cell to another. It is likely that enterprising companies will find ways to capture the unique identifier transmitted by cellular phones. Being able to link the cell phone's unique identifier with the true identity of the cell phone user would be a major advance in location-tracking capability -- and one that we are likely to see.

Recent Applications

A Connecticut car rental company used GPS systems to track car renters' speed, fining one renter \$450 for allegedly speeding three times and deducting the money from his bank account without informing him. Acme Rent-A-Car had to refund money to 27 fined renters after an intervention from the Connecticut Attorney General and State Commissioner of Consumer Protection. But the incident showed how quickly wireless tracking technology was evolving.

Don Simmonds, president and CEO of AirIQ, said General Motors is the largest supplier of satellite global positioning technology in the consumer market with their On Star system, while AirIQ is the largest supplier to the commercial market. "We supply

technology packages from which fleet owners can select various forms of reporting,” Simmonds said. This includes programs which set off an alarm when a vehicle hits a certain speed, reaches a maintenance mileage, or the company’s “most popular service,” when it’s driven past a designated boundary, he added.

Loretta Waters, a spokeswoman for the Insurance Information Institute in New York, said if Acme's approach proves effective, it could earn a rate reduction for a rental car company. "Certainly anything that can reduce any propensity to speed would be something we would favor," Waters said.

The *Washington Post* reported August 23 that U.S. law enforcement authorities might soon expand the use of "Carnivore," the FBI's controversial e-mail monitoring system, to capture e-mail and other text messages sent through wireless telephone carriers.

The FBI may apply Carnivore to wireless messages because the industry has been unable to come up with a way to give law enforcement agencies the ability to monitor digital communications as they can the more easily captured analog messages, as required by the 1994 CALEA law. Carnivore, also known as DCS1000, is controversial because of its ability to capture massive amounts of electronic communications in the course of searching for a select few messages.

In warning about the FBI plan, CTIA General Counsel Michael Altschul said the FBI stated specifically that it would turn to Carnivore as early as October 2001 if the industry could provide a more targeted system. In an Aug. 15 letter to the FCC, Altschul said the industry was unable to meet that deadline.

Clearly, if the law enforcers have developed a system like Carnivore to broadly capture electronic communications, it will not be long before it can develop a system for capturing location data as well.

Spam. In Japan, where wireless service has thrived, NTT DoCoMo this summer offered customers free data access and other discounts to counter the costs and inconveniences caused by rapid growth of spam. NTT DoCoMo also filed court actions against 30 alleged spammers.

Security. Although more and more major organizations are turning to wireless Local Access Networks (WLANs) for communications and computing, the security for wireless networks is woefully inadequate, thereby placing increasing amounts of sensitive data at risk. The research firm Gartner Inc. recently predicted that, by the end of next year, 30 percent of enterprises will suffer serious security exposures from deploying WLANs without implementing the proper security. Moreover, the currently-favored Wireless Encryption Protocol (WEP) was successfully attacked by researchers from Rice University and AT&T Labs. The researchers concluded that "WEP is totally

insecure," and advised administrators to use higher-level security mechanisms such as IPsec, a set of protocols currently in wide use to implement Virtual Private Networks (VPNs). www.cs.rice.edu/~astubble/wep/wep_attack.html & www4.gartner.com/DisplayDocument?doc_cd=99228

In the Feb. 2001 issue of *Communications*, two leading experts list several software-based threats to wireless security, including malicious code and WML Script. Anup Ghosh and Tara Swaminatha, of Cigital, a Northern Virginia software-security firm, said a key solution is "to build security into the platform and applications themselves, rather than attempt to introduce security patches afterward." They also point out that cellular communications are particularly vulnerable because in roaming from cell to cell, they can easily wander into the zone that a potential interceptor is set up.

The recommendation by Ghosh and Swaminatha that security at the outset be built into the platforms and applications themselves" underscores the importance of the "Privacy Impact Assessment (PIA)." If companies, particularly equipment manufacturers, conduct the appropriate PIA, then they can more effectively and efficiently design platforms and applications that respect fair information practices, even anonymity.

However, by failing to conduct a PIA, companies can design, sometimes inadvertently, systems or technology that is highly invasive and which pose integral threats to privacy. In those cases, companies might suffer from bad publicity when their work is discovered, and have to take on the added expense of issuing patches or corrections, or worse, recalling the product.

Traditional Problems, Proactive Solutions

In a relatively short tenure, we have seen how both commercial and police sectors in the United States have demonstrated a willingness to exploit wireless and location-based technologies in ways that do not comport to fair information practices. Similarly, we have seen in Japan, the flagship society for wireless text service, how spam has emerged as a problem that significantly detracts from the service. The incentive to spam will only increase as the capability of location technology improves.

Possibly even more ominous is the evidence of glaring weaknesses in wireless data security. It appears that growing numbers of major organizations are relying on WLANs and other wireless systems to handle sensitive information without due regard for probable vulnerabilities. Moreover, location technology heightens the importance of wireless security, as it could be directly tied to physical safety in certain circumstances.

The emergence and inevitability of wireless systems underscores the importance of protecting Fair Information Practices in law, and of adequate enforcement mechanisms and remedies. The majority of Western nations, which have comprehensive privacy law and an independent privacy commissioner, have a better infrastructure in place to deal with the challenges posed by wireless location technology than nations that do not.

The wireless environment also demonstrates the limits of reactive solutions, like laws and after-the-fact enforcement, and the importance of proactive measures that require that privacy is factored in at the design stage of products, systems and technologies. Thus, it is necessary to move in the direction of requiring organizations to assess the privacy impact of the products, systems, technologies and applications that they want to introduce to the public.

Pollution of our air, water and overall environment made the Environmental Impact Statement a necessity of the industrial age. The growing threats to personal data and privacy posed by rapidly advancing information and wireless technology similarly make the Privacy Impact Assessment a necessity for the Information Age.

Evan Hendricks
Editor/Publisher
Privacy Times
P.O. Box 21501
Washington, D.C. 20009
(301) 229 7002
(301) 229 8011 [fax]
evan@privacytimes.com
www.privacytimes.com