NASCIO Representing Chief Information Officers of the States

Research Brief

August 2005

NASCIO Staff Contact: Mary Gay Whitmer, Issues Coordinator, mwhitmer@amrms.com or (859) 514-9209.

The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Part I

I. Overview of Wireless Privacy Implications

Jim, a state employee, checks the radio of his brand new 1985 Buick Riviera for a morning traffic report—everything's normal so far. Miles down the road, however, Jim realizes that he forgot his favorite BBQ chips. Hurriedly, he spins by the grocery store only to find an empty shelf where the BBQ chips should be. Making the best of it, Jim places a refill order on an existing prescription at the grocery's pharmacy counter. Back on the road, Jim finds a long line at the toll road because of drivers with incorrect change. Frustrated, he turns on the radio, dialing past the music of Bruce Springsteen and John (still Cougar back then) Mellencamp, only to miss important detour information. What Jim also does not know is that a very time-sensitive message is waiting for him on his desk. Once at work, Jim scrambles between meetings with colleagues and accessing and reviewing files on his new desktop computer with a massive 20 MB hard drive.

Fast forward twenty years. Again taking off without his BBQ chips, Jim's wife alerts him via his smart phone. This time, he finds his BBQ chips in plentiful supply. Radio Frequency Identification (RFID) tracking at the pallet level helps the grocery store stay well-stocked and also ensures that Jim's prescription does not contain counterfeit substances. Jim checks out quickly by waving his RFID payment key fob at the cashier counter. At a stoplight, Jim reads an urgent email on his smart phone. He then breezes past the toll booth in his silver Nissan 350Z Coupe without stopping. The toll booth's RFID reader automatically scans an RFID-tagged sticker on Jim's car and deducts the toll from his pre-paid account. Listening to Coldplay's new single, Jim receives a traffic advisory from his on-board telematics system. On time to work because his on-board navigation system guided him through a detour, Jim powers up his wireless laptop with the needed files and conducts a meeting in a colleague's office. Jim's use of a smart phone, wireless network and laptop do not compromise sensitive state information because of good security and privacy protection measures and training the state provided to Jim and his colleagues about the responsible use of wireless technologies.

Why Wireless Privacy is Important for State CIOs: Through the implementation of carefully crafted privacy policies and appropriate security measures, state CIOs can ensure that state employees like Jim benefit from wireless technologies without creating dangerous vulnerabilities that could expose sensitive or personal state information to unauthorized individuals.

NASCIO • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: nascio@amrms.com • W :: www.nascio.org

Privacy Issues Remain with Common Wireless Technologies: State CIOs address privacy concerns within the context of an environment where wireless technologies such as laptops and PDAs are now common in the state government workplace. More importantly, wireless access is now pervasive outside the workplace, making working without wires very attractive, however risky. Although they are now too mature to be "emerging" technologies, laptops, PDAs and similar devices still have unresolved privacy issues that must be addressed and thus are included in this Brief along with other truly "emerging" technologies such as RFID.

The Changing Nature of Work in a Complex Mobile Environment: The role of the State CIOs in introducing mobile technologies while ensuring the privacy of personal information on or transmitted by those technologies is becoming increasingly complex due to the ubiquitous nature of wireless in the workplace. The lines between the standard nine-to-five workday and leisure time have become blurred. Many employees can access the state network at anytime from anywhere. This opens up potential privacy risks by providing employees new opportunities to conduct business outside of the controlled state office environment. State employees also may purchase personal wireless devices and use them for both personal and business purposes. Conducting work wirelessly from anyplace, at anytime, requires increased vigilance so that citizens' personal information remains safe from unauthorized exposure.

Helping State Employees Maintain Privacy While Working "On The Go": With wireless technologies, state employees are now often connected to the office while in off-site meetings or traveling. In fact, many employees who are given mobile devices will be expected to regularly check and respond to email even while in meetings. State CIOs need to gauge the potential impact of wireless adoption and the mobility needs of the employees participating in the changed mobile environment. They also can facilitate the development and integration of new technologies, working practices, skills and training for employees to mitigate potential legal and privacy risks.

Examples of Wireless Privacy Concerns: With the benefits of the wireless conveniences that Jim enjoys, he must also make sure to protect his personal privacy as well as the privacy of citizens' information that he handles on a daily basis in carrying out the duties of his state government job. Examples of wireless privacy issues in both Jim's professional and personal lives include:

- **Wireless Transmissions:** As a practice, should Jim transmit any personal or sensitive information via a wireless device? Unauthorized individuals could intercept transmissions from his laptop, which could compromise the personal information of citizens.
- **Portable Wireless Devices:** Jim stores email and sensitive information on his wireless Personal Digital Assistant (PDA), which could be dangerous if he accidentally misplaces the device (and Jim tends to misplace things). How does the state's wireless policy address the protection of data in a mobile environment?
- **Use of Personal Wireless Devices for Business Purposes:** Is it wise to allow Jim to use his personal smart phone for both business and personal matters? Must Jim follow his agency's wireless policy with respect to the smart phone?

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org

- **RFID & Consumer Products**: Will Jim's BBQ chips, which involve RFID-tagging at the pallet level, soon be individually RFID-tagged at the item-level and tracked once purchased by a consumer? Is this a privacy concern?
- **RFID and Prescription Drugs**: Will RFID tags be used to tag prescription drugs? If so, will the tags be disabled before Jim leaves the store?
- **RFID & Transportation:** Could the information on Jim's RFID-tagged toll road sticker be accessed by RFID readers other than the authorized one at the toll road? Is any sensitive personal information on the tag protected by measures such as encryption?
- **Advertising Using Geo-Location:** Could a business track the location of Jim's GPS-enabled smart phone and send ads to the smart phone when Jim is in close proximity of the business?

Overview of Wireless Privacy Risks:

This Brief will address the privacy implications of wireless technologies that currently exist or are emerging in state government. ***Privacy risks associated with wireless technologies generally involve either the unauthorized exposure of personal or sensitive information (such as individual health information) or the use of such technologies in a way that may be perceived as invasive to individuals.*** Examples of potential privacy concerns are below. Many of these risks may be addressed with appropriate security measures that will be covered in Part II of this Research Brief series. Appendix A contains additional resources on wireless technologies.

Unauthorized Exposure Risks:

- **Unauthorized Access While in Transmission:** Unauthorized access to personal or sensitive information while it is transmitted via wireless networks or devices.
- **Unauthorized Access While at Rest:** Unauthorized access to personal or sensitive information while it is stored on wireless devices, including the exposure of information if a wireless device, such as a PDA, is lost, misplaced or stolen.
- **Exposure of the Wired Network:** Risk of a compromised wireless device being used to gain unauthorized access to information transmitted via the wired network.

Invasive Use of Technology Risks:

- **Tracking:** Using geo-location technologies or RFID containing personal information about individuals to "track" their whereabouts and relate that information back to the individual.
- **Profiling:** Using geo-location or RFID technologies to collect information over time and build "profiles" of individuals' preferences, locations or other characteristics.

II. Background on Existing and Emerging Wireless Technologies in the States

Wireless network and device technologies allow one or more devices to communicate without physical cabling connections and are now more common in state government. The following information on typical wireless technologies along with current or potential state applications is offered as background to understanding wireless issues (see Appendix B for more details).

Wireless Networks: Wireless networks allow computers, laptops, PDAs and other wireless devices to connect with each other and/or connect to the Internet without wire-bound

connections. These networks employ a variety of wireless transmission modes and protocols including global coverage using satellites, radio networks, cellular technology and even broadband. Types of networks range from structured Wireless Local Area Networks (WLANs) to more dynamic Bluetooth systems that connect devices that are within close proximity of each other. Wireless hot spots using Wi-Fi are becoming more common in public areas, such as airports, bookstores and coffeehouses, since they allow individuals to use their laptops, PDAs and other devices to connect to the Internet.

- Government agencies may use WLANs allowing employees and visitors to have Internet and applications access from anywhere in the office or public building.
- State employees who are "on the go" or working remotely may use wireless hot spots or Bluetooth networks to connect to state information resources via the Internet.

Portable Wireless Devices: These technologies place computing power, including email and Internet connections, in the hands of individuals who are "on the go" and may also incorporate cell phone capabilities within the same device.

- State employees may have laptops, wireless PDAs or handheld units for use "in the field" that allow them to access or enter data into a state network from remote locations for more efficient application management.
- If permitted by state policies, state employees may purchase their own portable wireless devices and use them for both business and personal use.

Geo-Location Technologies: These types of technologies, which include Global Positioning Systems (GPS), can be used to track devices such as PDAs and smart phones that are geo-location-enabled.

- States may use this technology to track work and emergency vehicles allowing for improved routing and efficiency.
- States may also use this technology to track employees and vehicle locations as both a risk management and an operations management tool.

Radio Frequency Identification: RFID is a tracking technology that works via an RFID tag attached to or placed within an object. The tag contains information about the object to which it is attached such as a unique identifier. An RFID tag reader communicates via a wireless radio network with the tag and can read the information contained on the tag. Cutting-edge uses include implanting an RFID chip below the skin of a pet. If lost, the chip would contain information to link the pet to its proper owner.[1] The U.S. Food and Drug Administration (FDA) also recently approved the use of an implantable RFID chip in humans for medical purposes. The chip would contain a unique identifier and would facilitate the retrieval of an individual's medical information that is linked to the identifier.[2]

- While state government use is somewhat limited to toll booths, building access and the tracking of cattle, prisoners and work-related vehicles, RFID can also be used to track other government assets, employees and shipments. Some states have considered proposals to

[1] "RFID: Cats! Dogs! Guitars?" PCMag.com, (July 13, 2004), <http://www.pcmag.com/article2/0,1759,1612809,00.asp>.
[2] VeriChip Products, <http://www.4verichip.com/verichip.htm>.

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org

include embedded RFID chips in drivers' licenses and vehicle license plates. The United Kingdom recently began conducting a pilot program to test RFID-embedded license plates.[3]

- Currently, the U.S. State Department is working on plans to place RFID chips in U.S. passports thus providing quick access to travelers' passport information and also is examining ways to address the privacy and security concerns that were recently raised.

III. Wireless Privacy Implications for States

Some privacy risks may be specific to a wireless technology, while others may be the same as those that threaten information in the wired world. Although this Brief's scope is limited to addressing the privacy risks associated with wireless in the state government workplace, the reader should note that there are many resources available to address security controls for wireless technologies (see Appendix A for additional resources). ***Part II in this Research Brief series will address security controls as well as privacy policy techniques to protect sensitive information from wireless technology's vulnerabilities.*** Part II is slated for release later this year and will be available at: www.nascio.org.

Unauthorized Exposure Risks:

Beware of the War Drivers--Exposure in Transmission: Maintaining the privacy of the content, as well as the security, of WLANs takes a level of effort exceeding that needed for wired technologies, since the transmission through the air instead of cables creates vulnerabilities specific to wireless technology. If not properly protected, it places the transmitted information at risk for access by unauthorized parties, creating the potential for identity theft of citizens' personal information.

The importance of ensuring that wireless networks properly protect personal information has been highlighted by a recent U.S. Government Accountability Office (GAO) report that found consistent shortfalls by surveyed federal agencies in protecting wireless networks and training federal employees on their proper use.[4]

Instances in which wireless transmissions might be intercepted and lead to the unauthorized exposure of personal or sensitive information include the following:

- **The Exploits of War Drivers:** Wireless networks may broadcast signals outside of the office building, thereby allowing hackers, known as "war drivers," to park in close proximity to a state office building with a laptop and intercept personal, password or other sensitive information transmitted over the network. The National Institute of Standards and Technology (NIST) has characterized this scenario as particularly easy to carry out via an analyzer tool used from a nearby parking lot or road, because WLAN security features typically are not enabled and numerous security vulnerabilities exist with the current standard for wireless technologies, 802.11.[5]

[3] "Brit License Plates Get Chipped," Wired News, (August 9, 2005), <http://www.wired.com/news/privacy/0,1848,68429,00.html>.

[4] "Information Security: Federal Agencies Need to Improve Controls Over Wireless Networks," U.S. Government Accountability Office (GAO), GAO-05-383, (May 2005), <http://www.gao.gov/highlights/d05383high.pdf>. Hereinafter, "GAO Security of Agencies' Wireless Networks Report."

[5] "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," Tom Karygiannis and Les Owens, the National Institute of Standards and Technology (NIST), Special Publication 800-48, (November 2002),

- **Rogue Wireless Access Points:** Unauthorized or "rogue" access points open an unsecured connection to the wireless network and bypass authentication measures to prevent unauthorized users from entering the network. If undetected, rogue access points can expose personal or sensitive information transmitted on the network.
- **Use of Default Configurations:** A wireless technology's out-of-the-box or default features may not be adequate to protect wireless transmissions from interception risks and may require implementation of more stringent security measures and configurations.
- **Wireless Hot Spot Connections:** Public wireless "hot spots" can also pose risks in terms of exposing personal information, since, by design, hot spots can be used by anyone. If a state-issued device that is not properly protected connects to a public wireless hot spot, then information transmitted by the device, including passwords and financial and other sensitive information, could be exposed. Consumers also should be cognizant of the risks posed by shopping online or conducting other activities via a hot spot connection without privacy and security protections in place.

Beware of Prying Eyes--Exposure in Storage: States' vast amount of citizens' personal information stored on wireless devices must be protected from identity thieves as well as from unauthorized employee snooping. ***An over-arching issue is whether a state has determined if there is personal or sensitive information stored on state-issued wireless devices.*** If so, then the state should determine through data classification if the information would be better protected on fixed, wired devices such as desktop computers that do not have some of the vulnerabilities associated with wireless technologies. Additionally, the storage of sensitive information for longer than it is needed creates inherent risks for the exposure of the information.

As with the risk of interception in transmission, a wireless device's default configuration may not adequately protect information stored on the device. And, even after proper configuration, there is a risk that an employee or a third party could install an unauthorized application or program on a wireless device that could lead to the exposure of personal information. For example, the inadvertent installation of a spyware program on a wireless laptop, even if unintentional, could allow for the easy extraction of sensitive information.

Because of their increasingly small size, smart phones and wireless PDAs, as well as slightly larger devices, such as laptops, are susceptible to accidental loss or theft. Recent news reports have highlighted the danger of storing personal or other sensitive information on these mobile devices, because, if compromised, individuals may be at risk of identity theft.[6] Depending upon the nature of their work, some employees may find substantial benefits in being able to check email remotely or enter data from the field into an application such as a case management system. ***However, employees who do not have a legitimate business need for such technologies (or for high-powered applications on their wireless devices) increase the risk that established wireless policies and protocols will not be followed or that the devices will be lost or stolen and result in privacy breaches.***

<http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf>. Hereinafter "NIST Wireless Network Security Publication."

[6] "Thief steals UC-Berkeley laptop," cnn.com, (March 9, 2005), <http://www.cnn.com/2005/TECH/03/29/stolen.laptop/>.

Since portable wireless devices typically may be used by employees for both business and personal use and may even be purchased by employees themselves, employees may not be as aware of the risks to sensitive information on those devices, as they are of such risks with their desktop computers. For example, employees may not know that the synchronization of a wireless PDA with a desktop computer could create vulnerabilities that can compromise sensitive information. NIST has even suggested that, as handheld devices have become more capable while shrinking in size, some agencies should consider prohibiting users from bringing them into their facilities if they pose a potential security risk.[7] Unauthorized access can even be carried out via a state-issued device by an employee who has either been terminated or resigned if the device is not immediately deactivated and access disabled before or after the termination or resignation.

Shut the Door—Exposure of Personal Information Transmitted on the Wired Network: Employees' use of wireless devices, such as PDAs, also can be a vehicle through which unauthorized individuals can gain access to personal information transmitted on a state's wired network. Devices that are not configured to securely navigate a state's Virtual Private Network (VPN), firewall and other protective measures, could serve as a back door for compromising sensitive information transmitted on a state's wired network. Particularly where a wired network has multiple entry points, it may be difficult to ensure the proper authentication of wireless devices before access to the wired network is permitted. Additional risks are created for states that have not examined the design of their wired networks in order to identify vulnerabilities that could be exploited by wireless devices.

Invasive Use of Technology Risks:
It's 10 AM--Do You Know Where Your State Employee Is? Tracking & Surveillance Concerns:

Geo-Location: Geo-location technologies, such as GPS-enabled smart phones or PDAs, can track the individual carrying the device in real-time or near real-time. ***The ramifications of these concerns can range from being perceived as eroding individuals' anonymity or right to privacy by revealing other personal information by inference (for example, if a person visits a specific type of doctor's office, one can infer personal medical information) to providing the means for a stalker or other person with malicious intent to locate a victim and cause serious harm.*** One caveat to these concerns is that the privacy implications of locator technologies depend, in part, upon the technology's accuracy in pinpointing location. However, the importance of privacy safeguards for location information likely will increase as the accuracy of location technologies improves. For example, in the future, sensor networks for mobile devices may have a level of accuracy within a few centimeters.[8]

State governments are increasingly dealing with privacy issues related to tracking and surveillance from a number of standpoints, such as state employees carrying location-enabled

[7] NIST Wireless Network Security Publication.

[8] "Privacy Issues in Location-Aware Mobile Devices," Dr. Robert P. Minch, Department of Networking, Operations and Information Systems, College of Business and Economics, Boise State University, (2004), <http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650127b.pdf>.

smart phones and PDAs with them. Some government agencies are equipping work vehicles with location technologies in order to effectively deploy resources, prevent employee downtime and improve productivity. In such cases, labor unions may raise concerns on behalf of their members as well. From a consumer perspective, individuals may not be aware that their personal wireless devices possess locator capabilities or that those capabilities may be engaged as part of a device's default configuration.

At the state level, there has been some limited regulation of wireless tracking technologies, particularly in the context of on-board vehicle location technologies. California was the first state to enact a law prohibiting the download of data about a vehicle's location or other information without an owner's permission or a court order. Both California and New York prohibit car rental companies from using electronic surveillance via GPS to impose fees, charges or penalties regarding a renter's use of a vehicle.[9]

RFID: Dating back to its initial use during World War II to distinguish friendly aircraft from enemy aircraft, RFID technology has, at times, incited passionate debate about its use and potential integration into our daily lives. ***While the details of this debate could fill volumes, states must realize that this is still a fledgling technology, particularly at the state level, that holds great promise as well as significant, whether real or imagined, privacy concerns.*** On the one hand, government's use of RFID can greatly improve security and accountability for physical and access control and tracking capability for objects, shipments, baggage on flights, documents, radioactive materials, evidence, weapons and other assets. A recent government IT executive survey by the Information Technology Association of America (ITAA) indicates that 56% of the surveyed executives describe RFID as an emerging technology that would greatly improve government processes.[10] Some innovative uses, however, such as implantable RFID chips with medical information for humans and RFID-enabled identification badges for school children have raised concerns about this technology's impact on individual freedom of movement and anonymity.

Even with the public debate, some federal agencies are implementing RFID to track government shipments and assets and incorporating the technology into U.S. passports.[11] ***States may choose to follow the federal government's lead with RFID applications of their own, including tagging state-issued documents, such as driver's or professional licenses, and government assets for tracking purposes.*** Current estimates indicate that widespread implementation of RFID technology is most likely at least five years away.[12]

According to a 2003 position statement on RFID issued jointly by a number of high-profile civil liberty and privacy organizations, RFID privacy concerns revolve around:

---

[9] "2005 Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles," National Conference of State Legislatures (NCSL), (August 11, 2005), <http://www.ncsl.org/programs/lis/privacy/blackbox05.htm>.
[10] "ITAA Agenda: RFID's Rapid Rise in the Government Space," Harris N. Miller, Information Technology Association of America (ITAA), (November 30, 2004), <http://newsletters.itaa.org/public/article.php?ID=1731>.
[11] GAO Security of Agencies' Wireless Networks Report.
[12] "Information Security: Radio Frequency Identification Technology in the Federal Government," U.S. General Accountability Office (GAO), GAO-05-551, (May 2005), <http://www.gao.gov/new.items/d05551.pdf>. Hereinafter "GAO RFID Report."

- The placement and use of RFID readers and tags without notification
- Unique identifiers assigned to all objects worldwide
- Massive data aggregation as a result of linking identifiers found on tags with personal and other information
- The proliferation of surveillance, tracking and profiling practices via RFID
- Whether the technology will be used in a way that reduces personal anonymity.

The organizations that issued the position statement oppose RFID-tagging at the item-level until further assessments can be conducted by a neutral party.[13] However, this view should be considered along with the fact that RFID readers generally emit radio waves at a certain frequency and only the tags that are designated to respond to that frequency can be located and scanned by the reader.

The federal government has been studying the use of RFID and its potential privacy impact. Two potential privacy concerns include:

- **Function Creep:** In May 2005, GAO issued a study on RFID use in the federal government and broadly recognized the concerns of privacy advocates. GAO also raised concerns about the potential for "function creep" with secondary uses of information collected from RFID tags. The GAO report said that, like the function creep that has occurred with Social Security Numbers, the problem is of a policy, not technical, nature.[14]
- **Unsecure Databases:** The Federal Trade Commission (FTC) has raised concerns that "many of the potential privacy issues associated with RFID are inextricably linked to database security" and warrant the implementation of "reasonable and appropriate" data protection measures.[15]

While RFID is currently not regulated at the federal level, state legislation remains a possibility in the coming years. For example, a bill is currently pending in the California state legislature that would severely restrict the use of RFID chips in identification documents issued by the state.[16]

We Know More About You Than You Know About Yourself—Profiling Concerns on the Horizon: With the increased availability of location information via mobile wireless technologies like location-enabled smart phones and RFID tags, privacy advocates and others have raised concerns that location and other information may be collected via these technologies over an extended period of time, then related to specific individuals and translated into profiles of individuals' whereabouts, tastes and preferences. By using location or other information, businesses may be able to create customer profiles in order to provide more tailored marketing. Moreover, businesses may seek access to location information from wireless

[13] "Position Statement on the Use of RFID on Consumer Products," Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Privacy Rights Clearinghouse, American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Junkbusters, Meyda Online and Privacy Activism, (November 2003), <http://www.privacyrights.org/ar/RFIDposition.htm>.
[14] GAO RFID Report.
[15] "RFID Radio Frequency Identification: Applications and Implications for Consumers," Federal Trade Commission (FTC), (March 2005), <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf>.
[16] "2005 Privacy Legislation Related to Radio Frequency Identification (RFID)," National Conference of State Legislatures (NCSL), (August 11, 2005), <http://www.ncsl.org/programs/lis/privacy/rfid05.htm>.

service providers so that they can send ad messages to cell phones that are within a close proximity of their place of business. Finally, because potential applications for location and RFID technologies are still being explored, businesses may try to collect more information via those technologies than is necessary in anticipation that the information may be useful for future applications.

While profiling concerns currently focus on businesses' use of location and RFID-tag information, states still may have to deal with profiling concerns related to government applications of wireless technologies that collect location information. Citizens may have concerns in terms of whether the government is storing that information, linking it to other personal information held in other parts of state government or using it for secondary purposes.

IV. Conclusion—Why It's the Year of Working Dangerously:

Working in the wireless world today can be dangerous without paying strict attention to privacy concerns. Below is a list of scenarios with potential privacy implications that, if not addressed, could outweigh the mobility and productivity benefits that wireless technologies bring to the state government workplace.

- Will war drivers parked outside a state office building be able to intercept sensitive information transmitted over the state's wireless network?
- Will a terminated employee retaliate against his former state employer by plugging his still activated state-issued wireless PDA into an office computer before he leaves for good so that he can take with him some personal information and engage in the criminal enterprise of identity theft?
- Will the state be able to stop a state employee from connecting to the state's wired network via an improperly configured wireless PDA that has the potential to allow a nearby hacker using the same public wireless hot spot to access the state employee's password information and gain unauthorized entry to the state's wired network and the citizens' personal information that is transmitted over it?
- Can the state reassure citizens as well as privacy advocates that the state work vehicles that are newly equipped with geo-location technology will only be used to facilitate increased productivity and better navigation and not just for the purpose of monitoring the movements of state employees?
- Can the state successfully protect any reasonable expectations of employee privacy while implementing a "contactless" employee ID card with the purpose of securing agency offices from unauthorized persons and facilitating employee access?

Part II of this Research Brief series will highlight privacy policy and security measures to assist states in examining and addressing potential privacy implications so that the integration of wireless technologies can continue to make state employees more productive in serving the citizenry without compromising privacy.

To be continued…

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org

Appendix A: Additional Resources

General:

NASCIO:

"Wireless in the Workplace: A Guide for Government Enterprises," NASCIO, (April 2004), <https://www.nascio.org/publications/index.cfm#Wireless2004>.

Federal:

"Wireless Network Security: 802.11, Bluetooth and Handheld Devices," Tom Karygiannis and Les Owens, National Institute of Standards and Technology (NIST), Special Publication 800-48, (November 2002), <http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf>.

"Securing Wireless Networks," Cyber Security Tip ST05-003, U.S. Computer Emergency Readiness Team (U.S.-CERT), (2005), <http://www.us-cert.gov/cas/tips/ST05-003.html>.

"Information Security: Federal Agencies Need to Improve Controls Over Wireless Networks," Government Accountability Office (GAO), GAO-05-383, (May 2005), <http://www.gao.gov/highlights/d05383high.pdf>.

"Wireless Privacy and Spam: Issues for Congress," Marcia S. Smith, Congressional Research Service (CRS), Library of Congress, (January 26, 2005), <http://www.ipmall.info/hosted_resources/crs/RL31636_050126.pdf>.

"Hearings on Wireless 411 Privacy Act," Committee on Commerce, Science and Transportation, (Sept. 21, 2004), <http://commerce.senate.gov/hearings/witnesslist.cfm?id=1315>.

"An Examination of Wireless Directory Assistance Policies and Programs," U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, (September 29, 2004), <http://energycommerce.house.gov/108/Hearings/09292004hearing1387/hearing.htm>.

State:

"Wireless and Mobile Computing: An Overview and Quick Reference for State Agency IRMs and Executives," Texas Department of Information Resources, (2002), <http://www.dir.state.tx.us/pubs/wireless/wireless.htm>.

Wireless LAN Policy, Idaho Information Technology Resource Management Council, (April 2002), <http://www2.state.id.us/itrmc/plan&policies/3530.pdf>.

Other:

"TrustE Security Guidelines, 1.1," TrustE, (May 2005), <http://www.truste.org/pdf/SecurityGuidelines.pdf>.

"From E-Government to M-Government? Emerging Practices in the Use of Mobile Technology by State Governments," M. Jae Moon, IBM Center for the Business of Government, (November 2004),

<http://www.businessofgovernment.org/main/publications/grant_reports/details/index.asp?gid=165>.

"Code of Conduct for Mobile Marketing," Mobile Marketing Association (MMA), (November 3, 2003), <http://www.mmaglobal.com/modules/content/index.php?id=5&submenu=conduct>.

"M-Government: The Convergence of Wireless Technologies and E-Government," National Electronic Commerce Coordinating Council (NECCC), (2001), <http://www.ec3.org/Downloads/2001/m-Government_ED.pdf>.

Locator Technologies:

"2005 Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles," National Conference of State Legislatures (NCSL), (June 28, 2005), <http://www.ncsl.org/programs/lis/privacy/blackbox05.htm>.

"Privacy Issues in Location-Aware Mobile Devices," Dr. Robert P. Minch, Department of Networking, Operations and Information Systems, College of Business and Economics, Boise State University, (2004), <http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650127b.pdf>.

"Adopted WLIA Privacy Policy (First Revision)," Wireless Location Industry Association (WLIA), <http://www.wliaonline.com/indstandard/privacypolicy.pdf>.

"Web Services Applications Brief: Liberty Alliance ID-SIS Geo-Location," Liberty Alliance Project, <http://www.projectliberty.org/resources/whitepapers/IDSIS_Geo_Location.pdf>.

RFID:

Federal:

"RFID Radio Frequency Identification: Applications and Implications for Consumers," Federal Trade Commission (FTC), (March 2005), <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf>.

"Information Security: Radio Frequency Identification Technology in the Federal Government," U.S. General Accountability Office (GAO), GAO-05-551, (May 2005), <http://www.gao.gov/new.items/d05551.pdf>.

"Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security and the Consumer," U.S. House of Representatives, Committee on Energy and Commerce, (July 2004), <http://energycommerce.house.gov/108/Hearings/07142004hearing1337/hearing.htm>.

Other:

"2005 Privacy Legislation Related to Radio Frequency Identification (RFID)," National Conference of State Legislatures (NCSL), (August 11, 2005), <http://www.ncsl.org/programs/lis/privacy/rfid05.htm>.

"Guidelines for EPC on Consumer Products," EPCGlobal (2005), <http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html>.

"Radio Frequency Identification Technologies: A Workshop Summary," National Research Council, Committee on RFID Technologies, (2004), <http://www.nap.edu/catalog/11189.html>.

"Radio Frequency Identification: RFID Coming of Age," Information Technology Association of America (ITAA), (June 2004), <http://www.itaa.org/rfid/docs/rfid.pdf>.

"Position Statement on the Use of RFID on Consumer Products," Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Privacy Rights Clearinghouse, American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Junkbusters, Meyda Online, and Privacy Activism, (November 2003), <http://www.privacyrights.org/ar/RFIDposition.htm>.

"Government Decision Makers' Guide to RFID Pamphlet," National Electronic Commerce Coordinating Council (NECCC), (2005), <www.ec3.org>.

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org

Appendix B: More About Existing and Emerging Wireless Technologies

Wireless Networks: Wireless networks have increased in popularity in both government and private sector organizations because of their scalability and ease of installation. Such networks also provide employees with the ability to use their wireless devices at many locations around the office, which can lead to increased productivity. Wireless hot spots and Bluetooth or similar ad hoc networks can provide employees with the ability to use their wireless devices when out of the office. Common wireless network technologies are:

- **WLAN (Wireless Local Area Network):** Connects wireless computers and other components to a network using access points placed in strategic places in the office. Employees can use their wireless devices throughout the network's coverage area.
- **Bluetooth:** A Wireless Personal Area Network (WPAN) used to form a dynamic network that many remote wireless devices within close proximity of the network (approximately 30 feet) can join and leave as needed. Those devices can share files, Internet connections, and applications and even synchronize with each other.
- **Wireless Hot Spots:** Access points for wireless connections that are frequently located in public places, such as airports, university campuses or even coffeehouses.
- **Wi-Max:** A wireless network that provides greater range and bandwidth than WLAN. Wi-Max is typically used where there is not a line-of-sight between the wireless device and access point and can be used for "last mile" broadband access.
- **Wi-Fi (Wireless Fidelity):** A generic term for the standards pertaining to the transmission of data over wireless networks.

Portable Wireless Devices: These give employees "on-the-go" better opportunities to stay productive and provide them with improved access to information, such as news and traffic reports.

- **PDAs (Personal Digital Assistants):** Wireless devices with office productivity applications that may include database programs, schedulers, synchronization with other devices, email, text messages and Internet connectivity.
- **Smart Phones:** Merge cell phone and PDA capabilities into one device.

Geo-Location Technologies: Geo-location-enabled devices can be tracked by location. PDAs, smart phones or even vehicles may be enabled with GPS (Global Positioning Systems) or similar geo-location technologies. Depending upon the technology used, the location may be highly accurate or limited to the location of the nearest cellular phone tower. Applications of geo-location technologies include:

- **Tracking:** Tracking employees and/or their work vehicles (such as ambulances) to ensure better productivity, reduce downtime and, for vehicles, improve fuel savings and routing.
- **Traffic Updates:** Traffic updates tailored according to a user's location.
- **Find Other Users:** On cell or smart phones, these services allow users to locate their friends who use the same carrier (similar to an IM "buddy list").

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org

- **Onboard Telematics:** Some vehicles now are equipped with vehicle telematics or on-board vehicle information systems that include onboard navigation systems or the ability to communicate driving data.
- **Mayday Systems:** Telematics "mayday" systems that notify a call center under certain circumstances, such as when an airbag has been deployed.

Radio Frequency Identification (RFID) Technology: RFID is a tracking technology that works via an RFID tag placed in or on an object. The tag contains information about the object to which it is attached, such as a unique identifier. An RFID tag reader communicates via wireless technology with the tag and can read the information contained on the tag. Tags may be passive (unable to initiate contact with a reader) or active (able to initiate contact with a reader) or even integrate sensor or "smart dust" technology to form a sensor network. Unlike bar codes or magnetic stripes, RFID tags can be read from a distance and do not need to be within the reader's line-of-sight. Applications include:

- **Tracking Government Assets:** Tracking of government assets, shipments and even employees through RFID-tagged ID badges.
- **Quicker Access:** Using RFID technology to allow RFID-tagged cars to pass automatically through toll roads or gas stations, while the appropriate fees are automatically deducted from the driver's account.
- **Lost Pets:** Implanting RFID chips in pets that contain the owner's contact information so that the owner may be contacted if the pet is lost.
- **Retrieving Medical Information:** Implanting RFID chips in humans that contain a unique identifier that retrieves the patient's medical information.
- **Tracking Consumer Goods:** Tracking pallets and cases of consumer products to ensure fresh products, quality medications and well-stocked shelves.

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org