Ubiquitous Security: Privacy versus Protection

Timothy K. Buennemeyer Randolph C. Marchany Joseph G. Tront
Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, Virginia 24061

Abstract - In the ambient computing future, security promises to be the foundational design feature that allows pervasive systems to protect personal information privacy. As fledgling pervasive computing systems gain a foothold presence in becoming more flexible and, at the same time, more invisibly interconnected, system users may have to trade privacy and protection to gain full entry into this new information-laden environment. This paper examines the current state-of-the-shelf security components, which predominantly overlay wired and wireless networks that will support next generation pervasive systems with a defense-in-depth approach. Information technology "best practices" are considered, and privacy concerns within typical networks are discussed. An examination of emerging privacy protecting technologies is presented, and Radio Frequency Identification (RFID) tags and legal concerns are discussed to portray the asymmetry of information flow in pervasive systems that can impact our personal information privacy.

Keywords: Security, Privacy, Pervasive, RFID.

1.0 Introduction

Our society is growing and adopting a more ubiquitous information-filled world with previously isolated systems evolving and being adapted to operate in completely interconnected networks. This full access to real-time public and personal data is a logical evolutionary step forward. However, the security of the individual's confidential information and our right to privacy is at stake.

It is extraordinarily difficult to apply a security policy to flaw-laden and previously insecure interconnected system architectures. System and software designers are historically slow to adopt security changes and then to make necessary investments to protect the systems. Most security measures are merely stopgap actions to keep the existing systems afloat. However, privacy concerns are now emerging as a critical aspect of next generation pervasive systems.

In the ambient computing future, security should be the foundational design feature that allows pervasive systems to protect personal information privacy. This mindset change will have a profound effect on future system designs and implementations.

The rest of this paper is structured as follows. Section 2 presents a background to security and privacy problems facing pervasive systems. Section 3 discusses today's security architecture best practices that can be applied to next generation pervasive systems. Many of these design actions are grounded in today's available technologies and will continue as mainstays for the foreseeable future. Section 4 presents some technical solutions for protecting information privacy. Section 5 describes RFID tag technologies and legal concerns that present privacy risks and potentially greater information sharing benefits. Lastly, Section 6 provides a succinct conclusion.

2.0 Background for Security and Privacy

Historically, security of networks has been an afterthought. The Internet existed for nearly 25 years before genuine consideration was given to implementing defensive measures such as antivirus software, spyware detection, firewalls, and intrusion detection systems (IDSs). Not surprisingly, pervasive computing environments are being developed, but privacy aspects of security are only receiving secondary consideration. More disconcerting is the fact that privacy problems are not capturing the needed design attention required to adequately protect users' information in existing networks and emerging pervasive systems.

In 2001, Satyanarayanan commented that privacy is already a thorny problem in distributed systems and mobile computing that is greatly complicated by pervasive computing. As users become more dependent on a pervasive computing system, it becomes more knowledgeable about that user's movements, behavior patterns, and habits [1]. Exploiting this information is critical to successful proactivity and self-tuning. Use of this information must be strictly controlled in order to

prevent a variety of unsavory uses ranging from targeted spam to blackmail. Indeed, the potential for serious loss of privacy may deter knowledgeable users from using a pervasive computing system. Greater reliance on infrastructure means a user must trust that infrastructure to a considerable extent. Conversely, the infrastructure needs to be confident of the user's identity and authorization level before responding to his requests. It is a difficult challenge to establish this mutual trust in a manner that is minimally intrusive and thus preserves invisibility. Privacy and trust are likely to be enduring problems in pervasive computing [1].

Many questions need to be addressed regarding the scope and volume of personal information that should be shared in pervasive computing environments. Seemingly, there is a tradeoff between exploiting the tremendous benefits of having shared information available to enhance the user's life and giving away one's personal privacy either directly or indirectly. Jiang stated that pervasive computing with its promise of ubiquitous sensing, invisible form factor, and persistent storage of data has the potential to become a serious threat to privacy [2]. Additionally, the noted legal expert, Lawrence Lessig, commented that practical privacy is shaped by four strongly interacting forces: market, social norms, legislation, and technology [2, 3]. Lastly, Jiang suggested that in order to successfully address privacy concerns, ubiquitous computing technology must be designed to minimize information asymmetry [2]. So if defensive systems and security strategies can allow necessary mutual trust while minimizing information asymmetry, then individual privacy can be protected in emerging pervasive systems. Toward that lofty goal, this paper considers security best practices that apply to today's systems and potentially to tomorrow's pervasive environments.

3.0 Security Best Practices

In this section, a discussion of security best practices for today's networks is addressed. These described defensive components will presumably be deployed in next generation pervasive systems as well. Building, sustaining, and enhancing pervasive systems will be a financial burden, which many companies will offset by integrating these emerging ambient systems into their greater corporate networks. At face value, this may allow for multiple use network efficiencies and cost savings, but full integration of pervasive systems may have the disturbing side effect of exposing privacy and personally controlled information to everyday Internet vulnerabilities and exploits. Next generation pervasive systems must employ defensive security measures upfront and throughout the depth of the system. Those best practice security measures are common in many of today's wired and mobile system architectures.

First, security systems and privacy controls must be built into the system design from the onset. The security aspects will be accomplished by computer network defenses in a layered approach. This defense-in-depth methodology affords information assurance while maintaining data integrity. Presumably in a pervasive environment, the user's system will only provide a modest defensive computing capability, so the user and their computing devices will rely heavily on the pervasive computing environment for security. Additionally, the user will have to inherently trust the pervasive environment to benefit from the ambient information, but this trusting nature raises the specter of user privacy and information leakage concerns.

The defense-in-depth of any system consists of layers of defensive measures which will create a secure pervasive enclave. The perimeter defenses will employ multiple layers of firewalls that will conduct "stateful" data inspection. Routers will complement these defensive systems by implementing strict access control lists to only allow access by exception rules. Additionally, the administrator must employ tightly managed sub-netting to ensure privacy within the network, which will effectively hide the pervasive user's personal information from outside entities and the public in general.

The addressing scheme will be masked from the public network and the Internet. This situation gives the system administrator reasonable assurances of data integrity but does not guarantee that system has perfect security. However, it does provide a sound basis for network system security. Additionally, trusted connections will link into the system behind the outer firewall in the outer trusted zone but will still have to pass the scrutiny that the inner firewall policy sets as an added layer of protection from compromise. The perimeter defenses with appropriately configured alternate routes can provide some protection against attacks in the same manner as described above, presuming that the trusted links do not become saturated.

Second, a pervasive demilitarized zone (DMZ) will provide access to data summations from personal digital assistants (PDAs), RFID tags, and other ambient information sources. In this case, read-access can be afforded to outside entities, but the data remains completely controlled. The web servers in the DMZ provide real-time access to data through a web interface, which will provide reasonable access in a controlled cyber environment. Ultimately, the DMZ servers are expendable, if the system were to be attacked. The DMZ servers merely reflect the collected data that is aggregated and stored in core database servers. This information would be alternately available via

application servers in the heart of the next generation security enclave to decision makers in charge of the central database, so no critical system resources would be lost. The network connections and DMZ will be equipped with several types of IDSs. Conventional IDS devices would monitor the traffic on the network links and in the DMZ, and host-based IDS would ensure that key files on critical database systems and DMZ servers were not manipulated. Additionally, other access and authentication devices and schemes can be employed to further complicate the defensive maze. The challenge is that pervasive devices may not be very robust, so they will rely heavily on the network environment for security.

The IDS implementation and monitoring is of critical importance in creating the layered effect for the pervasive security enclave. Usually, two or more signature-based IDSs will be employed as will host-based IDS agents to monitor critical intelligent devices within the enclave boundaries. This practice accounts for the signature-based nature of IDS technology and gives the security administrator additional tools to spot and defeat potential adversarial activity on the pervasive network. As an additional benefit, properly configured and deployed IDS sensors throughout the network often detect configuration problems and provide a basic forensic logging capability for the administrator that can point to network problems that, once corrected, create greater system performance efficiencies.

Third, best security practices also include applying appropriate security configurations for software and hardware, keeping up-to-date with patches and operating system upgrades, monitoring system and network activity, disabling unneeded services, enabling maximum auditing, installing internal and external defenses such as firewalls, routers, and IDSs, and raising user awareness regarding computer security and privacy issues [4]. The remaining best practice security measures are common-sense matters in modern information technology systems, but they still need to be emphasized as key components of a secured network. The individual servers and computers must be locked down using a stringent security policy. Additionally, the basic security complement of device specific software such as client firewalls, antivirus software, and even spyware scanners should be employed where feasible as a final layer of security. The software applications must be linked to update servers, so updates and patches can be pushed as needed.

One would presume the perimeter enclave defenses to be adequate, although the last line of defense is often the well-defended host itself. To achieve this state of security, invasive scans must be employed regularly to identify unpatched systems, and then the final step of deliberate patching or removing unpatchable systems in a timely manner must be enforced, else the system architecture invites potential compromise from preventable sources. Checking for vulnerabilities and system policy changes will be part of the daily routine for an administrator, which is a very proactive approach to defense-in-depth and ultimately will provide information assurance to the users of the system. Many of the devices in pervasive environments will use embedded software and proprietary operating systems in combination. This does not minimize the need for an aggressive patching policy.

Fourth, Di Pietro suggested that the pervasive environment will be dominated by handheld/wearable wireless (HWW) devices that will require frequent communication with other appliances which must remain transparent to the user [5]. As device size decreases and mobility increases, the challenges to secure the various devices and maintain the user's privacy burgeon. Clearly a balance amongst confidentiality, integrity, and availability is required in the wireless domain. As with any information environment, device constraints play a large factor in the security capabilities that could be delivered. Lastly, the primary security weakness in the wireless environment is the fact that communications use radio signaling such that a knowledgeable attacker could monitor, capture, and potentially inject traffic without being observed. This creates a situation where each wireless capable notebook computer, PDA, smart phone, RFID tag, and even wireless sensor device is its own first and last line of defense.

Current technologies are not yet mature enough to ensure the cyber security of today's networks much less to defend tomorrow's pervasive systems. To a certain extent, everyone will have to make do with halfway measures as today's networks evolve into pervasive environments because it is not practical to eliminate all security risks or to close all security vulnerabilities [6].

4.0 Technical Solutions for Protecting Privacy

Up to this point, this paper considered security best practices as they relate to existing wired and mobile networks. This section describes some of the complementary technical solutions that are now emerging to protect personal information privacy. Alan Westin, professor emeritus at Columbia University, defines privacy "as the right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others" [7]. The problem is that information gathering tools are not typically designed to support the user's right to privacy. Information gathering has become commonplace in the

World Wide Web and takes various forms from cookies, to meta-data sampling, and to direct online questionnaires. The ever increasing sophistication and deployment of information gathering systems contributes to the escalating scope of personal data misuse and inappropriate information sharing. In the pervasive computing environment, the user's information could be collected actively or passively without the user's knowledge, which tips the balance of information asymmetry in favor of information collectors at the direct expense of user privacy.

Bayardo suggested that cases of improper disclosure and outright misuse of personal information affect both individual and collective behavior, so technical solutions must be developed to help protect our privacy [3]. The challenge is to allow some data mining to enhance our lives while protecting our personal information at the same time. There are few tools for managing personal data privacy at present. However, more privacy protecting technologies are now being developed.

Today's privacy protection technologies fall into 5 general areas: Hippocratic databases, privacy policy encoding, anonymization, privacy preserving data mining, and information sharing across private repositories [3]. Hippocratic databases are conceptual in nature and inspired by the Hippocratic Oath. These databases assume responsibility for the privacy of the data they manage as a core tenet and employ 10 fundamental privacy principles. These databases automatically enforce privacy principles by checking tagged data and relating privacy information to authorized querying users only, which is strictly enforced based on the privacy policy. The database explicitly checks whether or not the user has access to the data fields and then allows only records having purposeful attributes to be accessed, thereby enforcing user opt-in and opt-out preferences.

Privacy policy encoding allows an organization to encode its data collection and use practices in an automated fashion. Users can establish a privacy profile that is automatically compared when they enter the environment. Presently, there are two notable examples of privacy policy encoding: IBM's Enterprise Privacy Authorization Language (EPAL) and the World Wide Web Consortium's (W3C) Platform for Privacy Preferences Project (P3P) [8]. EPAL allows privacy enforcement systems such as Tivoli Privacy Manager to enforce enterprise privacy policies [3].

More recently, the W3C developed the P3P initiative, which enables automated matching between privacy policies and user preferences. This initiative is emerging as an industry standard for providing a simple, automated means for users to gain more control over the use of personal information that is potentially collected at websites. It comprises a standard set of questions that cover most aspects of a website's privacy policy. This taken in context collectively presents a clear picture of how that particular site will handle personal information [8]. The idea is that an enabled system can automatically compare the website's privacy handling policy with the user's privacy profile. The user retains control of their information privacy based on their profile, and, more importantly, the P3P enabled system notifies the user in an understandable format, so they can make informed decisions whether or not to release additional information. This seems to be the first attempt to standardize and categorize personal information privacy in an interface format that is comprehended by both users and systems alike.

Anonymization tools are fairly common today, but they are typically web-based tools. In the future, these tools will evolve and then migrate into pervasive environments. According to Bayardo, anonymization will allow users the ability to deter organizations from collecting information about them in the first place, because this technology prevents data collection by hiding or blocking potentially identifying information [3]. In the pervasive environment, the user may connect to the system by a privacy proxy, which might allow a user to anonymously purchase items with no personal information being shared.

Privacy preserving data mining combines aspects of several emerging privacy technology areas. Anonymization can prevent companies from understanding their customer base and thus hinder efforts to improve their products and services [3]. Privacy preserving data mining would allow businesses to derive the required information for understanding client buying habits without collecting accurate personal information. Thus, businesses could collect information in an aggregate form for improving the services they provide but still keep personal information private by randomizing the individual's private information. This approach precludes the retaining of meaningful personal information about the user but allows businesses to build models of aggregate client information to optimize business decisions and gain higher level insights about their customers in general.

Lastly, information sharing across private repositories is a legitimate challenge because security policies will often not align perfectly between disparate databases. While consumers might, in some cases, choose to disclose personal information, they do not necessarily want the information they disclose combined into massively detailed consumer dossiers. When information is spread across these databases, the problem is to allow businesses to develop aggregate

models for information sharing without having to disclose individual privacy data [3]. In the future, multiparty database information sharing frameworks will need to be developed to achieve this ability to share information and still protect personal privacy.

In this section, we have described some existing and emerging technological solutions to allow information sharing and still protect individual privacy. "Technology alone cannot address all the concerns surrounding a complex issue like privacy, so the total solution must combine laws, societal norms, markets, and technology" [2, 3]. Clearly, by advancing what is technologically feasible and by addressing privacy concerns at the onset, we will be able to overcome the challenge of protecting individual privacy and then benefit from greater shared information.

5.0 Privacy and Legal Concerns with Technologies

Typically, new technologies are introduced within a business model that focus on capabilities and features being rapidly brought into the marketplace rather than fully considering security and privacy concerns. Today's emerging technologies such as RFID tags, E911 location-aware cellular phones, and other technologies pose a significant threat to personal privacy. "Location-aware technologies can theoretically create a trail of what you have been doing and where you have been doing it. If investigators bother to correlate information from different databases, the picture could be quite detailed" [9].

The challenge is that location tracking technologies are being rapidly brought into the marketplace, but there are virtually no state or national laws, regulations, guidelines, or policies in place to govern the use, potential misuse of these pervasive devices, or the correlated information that can be attained from these technologies. This section more closely examines RFID tags and considers some benefits and implications to personal privacy.

Location-aware technologies have tremendous potential benefits for the commercial sales industry. Location correlation is a critical aspect of merchandise inventory tracking and theft reduction for which RFID tags provide augmented information that can be monitored by retailers. Ultimately, the adoption of these technologies will provide substantial benefits. The benefits are twofold. First, the company will gain savings by better inventory management, reduced product losses, and presumably decreased labor costs. These advantages come at a relatively low price. Second, consumers will benefit as companies hold down product costs, which will be passed on in the form of attractive pricing.

So what is an RFID tag? According to Stanford, RFID tags are wireless, networked, pervasive computers, that are successfully integrated into their environment. They are easily attached, often of negligible weight and bulk, and offer many benefits for business, manufacturing, and tracking processes. RFID tags turn everyday objects into network nodes that uplink identity and status data to enterprise databases, storing new information as needed [10]. They literally vanish into commonplace objects such as library books, shipping containers, car keys, luggage tags, clothing, or even pets, offering efficiencies in handling, location, and condition tracking.

RFID tags fall into one of three categories as compared in Table 1. First, passive tags are categorized as having modest storage capabilities with constrained onboard read/write memory. Today's passive tags have limited transmission ranges for simple, fixed replies to interrogating readers through reflected energy from resonant circuits [10].

Second, active RFID tags have high-end onboard capabilities and can integrate analog and digital interfaces to the outside world. These active RFID tags go well beyond the basic functions of passive tags, moving into those of small wireless networked nodes. Furthermore, they have greater computing capability, provided by an onboard 8051 8-bit microcontroller, than first generation desktop personal computers did in the early 1980s. Third, hybrid RFID tags combine some of the capabilities of both active and passive tags. Differing from passive tags, some hybrid RFID tags have batteries that can boost their return signal strength and thus can be read at improved distances [10].

Clearly, RFID tags demonstrate tremendous potential to provide ambient information to the retailer, and there are certainly benefits for the consumer with tailored

Table 1. RFID tag characteristics comparison adapted from [10].

Tag Type	Memory	Reprogrammable	Processor	Power Source	Range	Reusable
Passive	ROM	No	No	RF	2 Meters	No
Active	RAM / ROM	Yes	8-bit	Battery	1 Kilometer	Yes
Hybrid	ROM	Yes / No	No	Battery	20 Meters	Yes

product marketing. RFID tags seem to be the first commercially viable pervasive computing product.

Luedtke raised concerns over the potential misuse of information carried in each RFID tag and its association with the customer once a tagged product is purchased. Unlike Universal Product Codes, RFID tags do not just identify a unique product rather they identify each unique instance of an item [11]. This situation creates marketing trepidations because RFID tags embedded in consumer goods could be potentially used for tracking information about the person's location and other private information based on combining the user's buying habits and the RFID tag's embedded data.

Luedtke commented that some states are considering a highway toll collection system using active RFID tags. While highway tolls are more easily collected, so too, can information about the individual's driving habits [11]. For example, the time between toll-booths can be measured to determine excessive average speed, which could present a situation where automated traffic tickets are issued based on correlated RFID tag and user information. In an effort to combat privacy concerns, many companies will encrypt RFID tag information. Moreover, RFID tags can be disabled or outright erased to eliminate the potential information leakage threat. He continued by stating that "just as the promise and potential of RFID tags are still being investigated, so are the privacy and security concerns still being identified and solutions being formulated" [11].

Interestingly, privacy concerns are being addressed at several levels with technological initiatives and by legislative actions. However, privacy and security issues will not be resolved by technical means alone. Much of the discussion concerning the tradeoffs between pervasive computing systems with free flowing information and the protection of personal privacy will be resolved by legislative initiatives, court rulings, and public opinion in our free democratic society. Recently, Senator Bowen of California held hearings to investigate RFID sensor usage. Senator Bowen was quoted as saying, "how would you like it if, for instance, one day you realized your underwear was reporting on your whereabouts" [12]? Senator Bowen is the chair of the legislative subcommittee on new technologies and is considered to be an advocate of consumer privacy. Givens, the Director of San Diego based Privacy Rights Clearinghouse, stated that "there has been scant scrutiny by policymakers on RFID sensors and pervasive computing and that these hearings are an important first step…because of the profound privacy and civil liberties implications" [12].

From a purely research perspective, the privacy concerns seem to be parochial. However, as previously discussed, the pervasive technologies are often developed first, and then security and privacy concerns are addressed in an appliqué manner. Clearly, pervasive technologies are going to be developed. Interestingly, when it comes to privacy, most people are presumably going to choose to retain control of their personal information. Many users will see the overriding benefits and then acquiesce. The greater concern, as addressed by Pottie of UCLA's Center for Embedded Network Sensing, is that "limits must be set on the use of technology because it is possible to setup these systems so that there is no privacy anywhere, moreover, the time is right for an assessment of this technology" [12]. At the end of the hearings, Senator Bowen was quoted as saying, "the goal of these hearings is not to create legislation that says this technology could never be used, but it is to gain a better understanding of the impacts of these new technologies" [12].

6.0 Conclusion

The proliferation of pervasive computing systems will continue for the foreseeable future, but left unchecked, these wonderful technologies can introduce many unresolved privacy concerns that are unknown to most users. Although a user's quality of life can clearly be enhanced by pervasive systems, the asymmetry of information flow may be detrimental to our free society. We must be careful that the potential surrender of private information does not override the benefits of emerging technologies. To this end, implementing well developed defense-in-depth systems to protect the pervasive computing environment is mandated. Most WHH computing devices are lacking in robust capability to protect themselves, so strong security must be built into the larger pervasive environment.

The asymmetry of information flow clearly favors commercial entities at present, so legislative and technological initiatives must intervene to set limits on the acceptable level of personal privacy information that can be shared within our societal norms. Else, we will repeat the mistakes that were learned as the Internet matured and users discovered that the Internet's dark element was more than willing to use any tool to undermine security to gain illicit information and cause havoc. Fledgling pervasive systems must be inherently designed with built-in security systems that address fundamental personal privacy issues upfront because of the high stakes associated with divulging personal information, which may ultimately amount to the surrender of our constitutionally protected right to privacy.

In 2001, Skoudis commented that it is hard to remember the world without the Internet. The systems were built in a much more innocent time, which assumed a collegial environment built for honest

researchers to share information. The Internet, along with the idea of people attacking systems for fun or to make a political point, developed so quickly that the systems have not had time to evolve into completely hardened systems they will need to be. In the meantime, it will be a constant struggle to try and stay ahead of the attackers [7].

These words reflect the parochial views that surrounded the development of the Internet, but it does not take a huge intellectual leap to substitute pervasive computing into the previous excerpt. Hopefully, researchers and technology developers will heed such warnings, and legislators will enact meaningful and timely laws that will protect our privacy and allow us the wonderful benefits that pervasive computing beckons.

According to MIT's Simson Garfinkel, a well known writer on privacy in networking and system security, we can preserve privacy in a networked world if we care enough to do so. After all, privacy in a networked world begins with our understanding and securing our own systems and networks. This will only become more important in the pervasive future, but system architects and designers will have to make this a fundamental part of the design goals, and citizens will have to insist that this be done [10]. The reality is that we can have personal privacy and protection in a pervasive environment. Mutual trust in pervasive system designs will require well thought out technical approaches that employ security best practices with emerging privacy enabling technologies. Those technologies are important and must fully enforce legal standards coupled with societal norms to achieve acceptable levels of privacy that we are willing to live with or without in future pervasive systems.

7.0 References

[1] M. Satyanarayanan, "Pervasive computing: vision and challenges," *IEEE Personal Communications*, vol. 8, pp. 10-17, 2001.

[2] X. Jiang, "Safeguard privacy in ubiquitous computing with decentralized information spaces: bridging the technical and the social," presented at the 4th International Conference on Ubiquitous Computing (UBICOMP 2002), Gotenborg, Sweden, 2002.

[3] R. J. Bayardo and R. Srikant, "Technological solutions for protecting privacy," *Computer*, vol. 36, pp. 115-18, 2003.

[4] G. Killcrece, Kossakowski, K.P., Ruefle, M., Sajicek, M., "State of the practice of computer security incident response teams (CSIRTs)," http://www.sei.cmu.edu/publications/documents/03.reports/03tr001.html, 2003.

[5] R. Di Pietro and L. V. Mancini, "Security and privacy issues of handheld and wearable wireless devices," *Communications of the ACM*, vol. 46, pp. 74-9, 2003.

[6] J. D. McDonald, *Electric power substations engineering*. New York, NY: CRC Press, 2003.

[7] E. Skoudis, *Counter hack: a step-by-step guide to comuter attacks and effective defenses*. Upper Saddle River, NJ: Prentice Hall PTR, 2001.

[8] W. W. W. Consortium, "Platform for privacy preferences project," http://www.w3.org/P3P/, 2002.

[9] J. Warrior, E. McHenry, and K. McGee, "They know where you are [location detection]," *IEEE Spectrum*, vol. 40, pp. 20-5, 2003.

[10] V. Stanford, "Pervasive computing goes the last hundred feet with RFID systems," *IEEE Pervasive Computing*, vol. 2, pp. 9-14, 2003.

[11] J. Luedtke, "Toward pervasive computing: RFID tags: pervasive computing in your pocket, on your key chain and in your car," DM Review, http://www.dmreview.com/ article_sub.cfm?articleID=7096, 2003.

[12] A. Gilbert, "Privacy advocates call for RFID regulation," CNet News, http://news.com/2100-1029_3-5065388.html, 2003.