

IN THE FEDERAL TRADE COMMISSION OF THE UNITED STATES

IN RE
THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND:
EMERGING TECHNOLOGY AND CONSUMER ISSUES
A Public Workshop

RESPONSE STATEMENT FOR DAY II PANEL:
Building Privacy and Security Solutions into the Technological Architecture

Gregory A. Miller
Chief Privacy Officer &
Vice President Corporate Development
MEconomy, Inc
1207 Indiana Ave Suite 1800
San Francisco, CA 94107
gam@meconomy.com

11.December.2000

I. Introduction

Mr. Chairman, Commissioners, Commission, and the Bureau of Consumer Protection: My name is Gregory Miller. I am an Internet business strategist whose 20-year career blends education and experience in technology, business, and law. My professional pursuits have tracked the evolution of the Internet from the days of the Arpanet to the engine of today's digital economy. My accomplishments are divided between software engineering and marketing/business development, with experience as a technology lawyer and an Internet public policy specialist. I have previously served on an FTC special committee for consumer online privacy and act in an advisory capacity to US Senators on matters of Internet policy. I also serve on the public policy committee of the Critical Infrastructure Assurance Partnership. In the private sector, I currently am the Chief Privacy Officer and Vice President of Corporate Development for MEconomy Inc. In this capacity, I am charged with ensuring MEconomy's product strategies fully support best practices and current laws governing consumer privacy. As a member of the executive management team I participate in setting business strategy and developing strategic alliances and relationships. This includes serving as MEconomy's thought-leader on consumer Internet privacy and security and liaison with government. My complete curricula vitae are incorporated by reference herein.

MEconomy is an emerging technology upstart company whose business is rooted in providing the technology infrastructure of an *assured privacy layer* ("APL") for the Internet. This APL will work across all delivery channels, wired and wireless. Within the context of the wireless medium – the focus of the FTC's research inquiry herein – MEconomy will offer an innovative technology for wireless gateway providers and intermediaries, among other types of service providers in the digital economy. MEconomy's system will offer an Infomediary that creates, maintains, and protects device, location, user, and service profiles. This Infomediary will empower the consumer to directly control their own data while allowing them to authorize the use of their data – giving permission to destination sites and other service providers – for specific and pre-identified purposes on an "opt-in" basis. MEconomy currently has portions of its software infrastructure in "alpha" and "beta" testing phases, and expects to launch a production-ready commercial-grade solution in the second quarter 2002.

On behalf of MEconomy and myself, I wish to extend my gratitude for being selected for this FTC undertaking and the opportunity to participate. The Federal Trade Commission has provided a set of issues and questions pertaining specifically to the building of privacy and security solutions into the technological architecture. On behalf of, and representing the business interests of MEconomy, Inc, as respondent and panelist member I respond to those questions for the record herein, preceded by a brief wireless industry background statement to set the background for my answers.

II. Wireless Industry Background Statement

The convergence of voice and data with delivery across a wireless medium should affect many sectors of the economy. I believe that a major software infrastructure will be required in the telecom sector to manage, route, and filter this traffic as it converges. Entirely new software applications and services will be developed to empower wireless users. Of course, within this infrastructure there must be new layers to manage privacy and security. Therefore, I offer the following observations as a backdrop for the answers to the questions posed by the Federal Trade Commission about privacy and security solutions into the technological architecture.

- **Infrastructure** – The first wave of wireless data services will be the infrastructure itself. With any emerging platform, the first wave of investment is typically in the underlying infrastructure that is required to deploy services. We are hopeful that a component of this will be privacy and security mechanisms that foster trust within eCommerce delivered across the wireless medium. I believe the wireless infrastructure build out will continue for the next 12 to 18 months.
- **Corporate Focus** – Over the next 12 months the focus should be on the corporate market rather than the mass consumer market. In the next 12 months the market will likely be driven by early adopters, and I believe that the mass consumer market will not significantly contribute to adoption for at least a year due to the lack of compelling content and applications. I could add the lack of privacy and security to that observation; however, consumers have little reason to give significant thought (yet) to the degree of privacy and security that lies in their mobile device. Once digital wireless devices entered the market, the general scare of analog wireless devices being “jacked” by telecom criminals standing on overpasses of major thoroughfares using technology available over the counter, the concerns of trust in the system integrity largely disappeared. As will be disclosed in my answers *infra*, this lack of concern (or awareness) likely will change as fresh light is shed on the blatant vulnerabilities of the current digital infrastructure integrity. However, for the next year, the focus will largely be on services provided in the corporate setting – I believe largely because of the market’s recent scare about the adoption risk inherent in subscription-based business models. Market research and analyst reports suggest that carriers are developing wireless services to offer to their enterprise customers over the next six months in an attempt to drive revenues prior to consumer adoption. It is during this stage that efforts should also be plied in the lab to bring about orders of magnitude improvement in system integrity for consumer privacy and security when that adoption begins.
- **Growth Challenges** – Over the next 12 to 18 months wireless data services adoption rates, usage patterns and revenue models will vary by geographical region. This is due in part to the frustrating state of standards in the United States compared to elsewhere on the globe. And I do not believe that Japanese NTT DoCoMo’s wireless data penetration, which was initially driven by entertainment applications, should be used as a proxy in the United States.

- **Market Adoption** – Wireless data services represent a large market opportunity, but there will be roadway hazards along the journey to profitability and wide-scale adoption. Worldwide cell phone subscribers are forecast to increase to more than 1.6 billion by 2004 up from 475 million in 1999, representing a 28% CAGR, and worldwide wireless data subscriptions will increase to more than 400 million by the end of 2004 up from approximately 15 million at the end of this year, 2000, representing a 127% CAGR [1]. However, I believe that this subscriber penetration could be adversely affected by technological constraints, lack of compelling applications, and most importantly, renewed fears of lack of device privacy and security, or system integrity.
- **Application Trends** – There will be a dramatic difference between wireless and desktop Internet applications. Wireless data services must be tailored specifically to the wireless device, and different devices will serve different markets. Location-specific services will likely permeate all wireless data services, similar to the ubiquity of search engines for the web on the desktop. Along these lines I believe five trends will emerge: 1) the convergence of voice and data; 2) growth of personal information management applications; 3) improved synchronization technologies; 4) optimized delivery platforms; and 5) an explosion of location-based services.
- **Success Attributes** – There are four attributes for success of wireless data services: ubiquity, integration, utility, and simplicity. And much of the functionality of data services will be made possible by voice-enabled technology (e.g., TellMe Networks – <http://www.tellme.com>) because today's 475 million wireless devices are optimized for voice communications, not data.
- **Technology Constraints** – The wireless Internet experience will be constrained over the next 18 to 24 months. The desktop is a powerful platform for information gathering, research, and commerce. Building privacy and security infrastructure around that is comparatively easy. However, the wireless platform is constrained by several factors including: lack of processing capabilities, limited bandwidth, network latency, limited user interface real estate, limited user input capability, the slow transition from switched to packet data transmission, closed carrier platforms and multiple standards, and limited applications.
- **Customer "Ownership"** – Some bristle at the use of the term "ownership" in conjunction with the word "customer," however, the fact remains that existing desktop brands and new entrants will compete with carriers for customer loyalty. All are likely to have to share revenues, as the platform becomes mainstream and transaction revenues begin to channel through the wireless medium. I do not believe the leading desktop brands such as Yahoo, [Excite@Home](#), or NBCi will become dominant wireless Internet brands unless the content and services they offer quickly scale and tailor to the constraints of the wireless platform outlined *supra*.

1 See Thomas Weisel Partners Wireless Infrastructure Analyst White Paper, Matt Finick, 28.August.2000

III. The Specific FTC Questions & Answers

1. Are there basic principles of technology and design that have emerged in the Internet space that can be applied in the wireless context to increase privacy and security?

For example, consider the basic principles of minimizing the degree to which data is personally identifiable; keeping information in the custody of the consumer to the extent possible; making data flows transparent/visible to consumers; encryption of all data and meta-data; minimizing data collection and retention; and decentralization of databases.

From a practical and policy standpoint the principles of technology and design that have emerged to manage or increase security and privacy are not always in parity with the same ones that have been adopted by the mainstream, and this is discussed *infra*. Further, there is not, in our opinion, a discernable amount of empirical evidence that the principles cited in the example above or some principles we add below have “*increased privacy and security*”. For example, giving consumers “*complete control of their information*” is a noble concept, but we do not believe there is sufficient evidence to conclude that this directly increases any privacy or security.

With that in mind, here are five principles, or perhaps goals we believe are worth consideration for privacy and security in the wireless infrastructure:

1. The user’s direct access device (e.g., wireless appliance, etc.) should be the initial source of encryption, and it should be performed end-to-end, *only* with trusted intermediaries.
2. The end device should be an open platform so users can load (or unload) their own privacy/security technologies.
3. All technologies that directly and initially touch consumer’s data (e.g., at the point of collection) should be available for unfettered public review (i.e., we support open source initiatives).
4. Consumers must have complete control over their information (e.g., fair information reporting principles of notice, consent [2], access, etc.).
5. Any data collected for a transaction should be de-coupled from personally identifiable data, and only used for that transaction.

We believe that by and large, consumers are not completely aware of the potential problems with privacy in a digital economy (e.g., identity theft, discrimination, crime, etc.) until a disaster strikes home. [3]

Likewise, consumers want a transparent experience that they can trust and rely on. For instance, by and

2 The concepts of “*choice*” and “*consent*” have been interchanged in recent literature. The respondents recognize that “*consent*” suggests an “*opt-in*” strategy, whereas “*choice*” could be either. We’re further appreciative of the fact that mobile commerce may become heavily weighted with financial services offerings. And under provisions of Graham Leach et al legislation the strategy is clearly “*opt-out*.” We recognize this may create an impasse – one the FTC should plan on addressing sooner than later because the public policy momentum appears to be building within the wireless business sector to support “*opt-in*” strategies.

3 Although unproven in the marketplace as yet, we further believe that an adopted Infomediary acting as the consumer protectorate

large, the lock icon that has become a fixture of web browsers to indicate that data is transferred securely has become a visual cue that requires no further intervention by the user (save a mouse click to acknowledge an alert panel). We believe a similar approach needs to be taken with regard to privacy – creation of an “*assured privacy layer*,” if you will. However, this discussion with regard to privacy in the context of the World Wide Web is significantly impacted by the constraints of the wireless medium. So we need to consider this question in light of the technical landscape of the mobile or wireless channel.

From a technical standpoint, good security requires the right tool for the right job. In other words, we need to use the proper application of the most effective protocols and processes. The four corners of consideration include:

- User interfaces
- Processing power
- Memory
- Bandwidth

Arguably hardware innovations have not arrived faster due more to business challenges than technology limitations. Likewise, the state of wireless security is less conditioned on hardware limitations and more on externalities explained *infra*. At the same time, we find that wireless application developers are asked to implement security capabilities suitable for desktop computing but not ready for wireless devices due primarily to these four architecture elements *supra*. As hardware improves, we believe security mechanisms may likewise improve, assuming we can circumvent the business and political challenges.

The most promising cryptography scheme for wireless clients appears to be ECC (Elliptical Curve Cryptography), a variant of public key cryptography algorithms. Strictly speaking, it is still under technical review, but is considered promising and industry consortia like the SECG are actively promoting implementation of ECDSA in mass-market products.

ECC provides security (and ECDSA provides authentication) comparable to that of RSA or Diffie-Hellman (of which the Elgamal variation is most widely used for encryption). The security of the hardware is still an issue, but that is continuing a problem with mobile systems that rely on discrete hardware to store secrets.

[4] Let's consider each point in the example provided by the Commission.

- **Minimizing Identifiable Data**

In terms of "minimizing the degree to which data is personally identifiable," Pseudonymization (e.g. AMEX' "Blue" card) is becoming "acceptable" in the business world and could become

would go a long way toward increase privacy and security.
4 Due to power/timing attacks on the key schedules.

commonplace in 2-4 years. This is because technically speaking; pseudonymity is built from security primitives with “provable” characteristics. [5] Pseudonymized networking protocols (e.g. Zero Knowledge Systems re-mailer) in some winning format (not necessarily Zero Knowledge Systems’ solution), will be widely used. Law enforcement will always seek over-access, creating healthy tension that drives the technology curve. For political and economic reasons, we believe that the EU will be a primary catalyst for this tension.

- **Keeping Information in the Custody of the Consumer**

Custody is important, but we believe the custody issue goes to more to the keys than the data itself. We believe one reason the security community rebuffs policy proposals for any form of key escrow is the concept that the root of privacy lies in the custodianship of the keys. In other words, keeping one’s keys anywhere but with the individuals themselves proffers compromise on its face.

- **Making Data Flows Transparent/Visible to Consumers**

We believe it is more important to make the security mechanisms transparent than it is to making the data flows visible. And we believe this is a driver for an increasing trend to place security software in an open source environment, subject to peer-review and full disclosure. The real issue, we believe is making certain data transport mechanisms are actually as secure as purported (rather than – for example – making certain a clickstream is opaque). To quote a former U.S. President, “*Trust and verify.*”

- **Encryption of all Data and Meta-data**

Encrypting data is a good measure, however, the challenging part, and the real focus ought to be verifying that the authorized individuals and only those authorized have the necessary keys. Assuming, however, that key management is properly maintained, encryption of data should be a business and/or utility proposition, predicated on the corresponding issues of ease of access, overhead, usability, performance, cost, etc. Simply encrypting all data will not solve the challenges of data protection, and in particular, the real issue is key management and security.

- **Minimizing Data Collection and Retention**

The Internet has provided a means for new levels of surveillance, unprecedented capabilities in direct marketing, and innovative approaches to customer care. And there are charges that what has evolved is more than a commercial Internet, but a global surveillance system of national and international security import. As a result, regardless of which purpose one subscribes to, the most difficult adversary may lie beyond unwanted direct marketing. It may lie within the constant tension that strains the relationship between individual privacy and the government’s charter to protect its nation. These practices are increasing (e.g., see the Walsh Report).

⁵ By “provable” I mean to suggest that technical proof notwithstanding, eventually, policy makers realize that mathematics works.

We believe that data collection should be minimized to purposes that must be disclosed. However, philosophically, we believe it is equally important to be wary of technologies and infrastructure that can be (and in some cases are) deployed for surveillance purpose – particularly where there is no clear and present need under well settled federal wiretapping and eavesdropping statutes. And regardless of whether technology is being deployed for such purposes by law enforcement or government agencies, we must be mindful of the illegal deployment of such technologies.

Therefore, when considering data collection and retention – regardless of the medium, wired or wireless – it is perhaps first and foremost to consider the regulation of data collection and retention. Currently, there is no regulatory or statutory scheme to minimize data re-marketing. We do not mean to suggest that regulation is the answer to all of the privacy and security issues or questions, however, we're also mindful that in some instances an appropriate mix of industry initiative and government support is in order.

- **Decentralization of Databases**

Centralization is a difficult proposition to resist, but peer-to-peer technology may be the natural antidote. Distributing data with strong crypto protection may afford a competent, feasible, and consumer comforting solution. Consider how gateway providers and intermediaries might maintain the aggregate data they want and need to render their services, but allow the actual profiles to remain directly in the control of their rightful owners – the consumer. On the other hand, in some settings, this may prove less than practical. Accordingly, we believe it comes down to having a strong trust relationship. If a trust relationship exists, then the aggregation of data into centralized databases may not be a pressing matter.

2. How are companies wiring in privacy and security today in the wireless medium? Are the protections currently employed adequate?

Simply put, we believe companies are racing to incorporate security advances that we believe are not being completely analyzed for security integrity. And as a result, the current employed protections are inadequate.

The supporting authority for this answer is highly technical. An overview is incorporated *infra* for the Federal Trade Commission's reference. Verification of the assertions below may be found in the literature or through review from security experts. Accordingly, the following details are based on descriptions provided by security experts whose general knowledge exceeds that of the author, but is readily available in the technology literature.

Generally, we believe the protections currently employed attempt to strike a balance between “breakability” for government intelligence agencies and sufficient security to thwart casual intercepts, and are reasonably justified by limitations in the technology (the four corners of consideration outlined in Question 1, *supra*).

For example, some academic cryptanalysts have argued that the ten+ zeroed-out bits in the A/2 and A/5 ciphers specified by the GSM Consortium is a classic example of this, although the wireless telephony industry denies this report. Add to this that the wireless security landscape has arguably changed dramatically in the past decade. Powerful cryptanalytic capability is so widely available in the intelligence world that it has naturally percolated down as publicly available computing techniques and inexpensive but powerful hardware. In fact, the types of intrusions that can be performed by relative amateurs have admittedly surprised law enforcement agencies from time to time, but they shouldn't.

One initiative containing these trapdoors includes WTLS, a wireless implementation of the Transport Layer Security (currently with known security flaws that competent security experts can explain). In the authentication area there has been good work using sufficient key lengths, such as the use of ECDSA (Elliptical Curve Digital Signature Algorithm) in wireless protocols for authentication. The key lengths are not foolproof of course, because any good authentication algorithm can *also* be used to encrypt (e.g. the Elgamal encryption variation on the Diffie-Hellman key exchange protocol).

TLS and WTLS bear a close resemblance to each other because the WAP Forum incorporated large sections of the TLS Working Group's protocol work directly into the WAP specification. This was a useful step to facilitate rapid development of the wireless medium and push the specification forward. However, the WAP Forum arguably also introduced several major cryptographic vulnerabilities to TLS. These compromises may be due to standard design constraints on wireless systems including:

- Mobile unit processors lacking power and memory capacity
- Bandwidth limitations
- Export restrictions on cryptography (as a market penetration factor)
- Common long round-trip latencies
- Lack of support for both connection-oriented and datagram transport layer protocols

Diving deeper into the technical details, the results are weaknesses in current wireless protocols using implementations of the WTLS security schema (e.g., WAP). Specifically, security experts claim that adding support for datagrams, optimizing the packet sizes for poor quality wireless environments (e.g., limited bandwidth) and specifying faster algorithms all introduced weaknesses to several well-documented attacks, including the following:

- WTLS reduces the key space by a factor of 32 from 40-bit DES by using 35-bit DES encryption to make it weaker and thus more exportable. 56-bit DES has 8 bytes of keying material, and therefore, we believe WTLS is unable to meet its own requirements for "best possible security."
- Another more serious allegation regards the "record_type" field. This data field is sent in the clear, so key changes could be eavesdropped and substituted. One example is the "ChangeCipherSpec" field. An attacker could turn encryption off by switching an unsuspecting owner's WTLS enabled device to a null cipher without the owner's knowledge. If true, this is a serious security flaw.
- Another allegation is that alert messages are sent in the clear and unauthenticated. Since they're given a sequence number, an attacker can – without detection – selectively replace encrypted datagrams with unauthenticated plain-text alerts by assigning the same sequence number. The result is what is referred to as a "truncation attack" where arbitrary packets can be dropped from the data stream selectively, or more sinisterly, replaced with others.
- Block ciphers are used in CBC mode (cipher block chaining), but WTLS uses a 40-bit XOR message authentication code (MAC), which "pads" message blocks with zeroes and then divides it into 5-byte "blocks" to be "XOR-ed" (a mathematical recombination process). Regardless of these short key lengths, this use of a weak XOR MAC in the stream (block) cipher in this manner provides no integrity protection.
- The block ciphers in WTLS are highly vulnerable to "brute force" attacks. To find the correct key, an attacker runs a trial decryption on the final block of each packet. Given the inexpensive processing power of laptops and other small devices commonly available today, brute force attacks no longer require a roomful of compute power.
- WTLS specifies Diffie-Hellman key agreement computations using 512-bit and 768-bit primes with generators, but it does not specify the group order generator of the multiplicative subgroup. This suggests one cannot check if the given public value belongs to the correct subgroup, which means an attacker has a backdoor if they want to mount a "factorization" attack. This RSA encryption is vulnerable to chosen "cipher-text" attacks. Security experts allege that cryptanalysis can be successful in approximately 2^{20} rounds – insignificant by today's commonly available compute power – because the RSA signatures and encryption conform to PKCS#1 v1.5. That standard provides an oracle that reveals if the correct padding is present on any given packet. And some WTLS implementations have error messages like "bad_certificate" and "decode_error" that can easily provide an attacker with precisely such an oracle.

In summary, chosen plain text (data recovery) attacks, datagram truncation attacks, message forgery attacks and "exportable" key space searching shortcuts, are all serious privacy problems buried in the technical details of today's digital wireless device implementations using WTLS v1.0. WTLS v1.1 has not remedied any of these allegations. The new specification implicitly suggests solutions, but fails to

implement them (e.g., SHA as an algorithm for handshake protocol).

Unfortunately, a similar story exists with the GSM security specification [6]. It is alleged that 150+ million GSM users worldwide are subject to eavesdropping, spoofing, cloning and hijacking and every single major GSM provider have been less than forthright about the sufficiency of security, marketing PCS devices using GSM technology as “secure” (e.g., Pacific Bell, a subsidiary of SBC). Arguably, some experts may counter that the security breach potentials outlined herein and alleged in the literature are so deminimis as to (as a matter of business decision and strategy) not be worthy of resolution at this time. However, there are security experts who claim to have seen demonstrations of commonly available desktop hardware and software technology that cryptanalyze and clone a PacBell PCS/GSM phone within 3 hours.

To take this one step further, we believe this form of identity theft is simply waiting to happen. Consider that the cloning approach mentioned above can also be deployed as a masquerading “base station,” so an attacker could sit in a convenient public location, and abscond with the A/5 keys of every PCS phone user who passed by talking on their PCS device and within a few hours, have cloned their phone. Security experts allege this to be true in the face of PacBell staunch denial, but regardless of what is the truth, we believe there is enough in question among reasonable persons to call for a deeper audit of current security architectures before any policy or regulation is fashioned.

3. Are there additional existing technologies that could build privacy and security protections into the architecture of wireless devices and services (For example, XNS or others)?

We first note in passing that XNS looks most promising. In general, however, we believe wireless privacy and security is not a technical problem, but more of a political problem. For example, the IETF (Internet Engineering Task Force) IPsec working group, the ANSI (American National Standards Institute) X9.F1 working group and the IEEE (Institute of Electrical and Electronic Engineers) P1363 working group have adopted Diffie-Hellman (X9.42), TripleDES Modes (X9.52), and ECDSA (X9.62, an elliptic curve version of NIST's Digital Signature Standard). Meanwhile, the wireless industry is still waiting for the WAP Forum to specify strong security mechanisms that overcome the current alleged deficiencies. We believe that if the current protocols had all the alleged weaknesses addressed, in conformance with the repeated recommendations of the academic and technical security communities, 95% of the most serious privacy vulnerabilities would be removed.

On the other hand, resolving these vulnerabilities would make law enforcement and other government

6 For details on these vulnerabilities see <http://www.scard.com> regarding GSM vulnerabilities particularly concerning the US version of GSM.

agencies' work more difficult – the political counterbalance. As a result, we query whether millions of wireless device owners use weak devices because there remains a threat of bad actors relying on the wireless medium to perpetrate their misdeeds. Unfortunately, if so, then this situation twists into an irony because the ability to compromise the existing security infrastructure is now within the reach of amateurs.

4. What kinds of technologies, standards or models may emerge to safeguard privacy and security in the wireless area? How far away are they?

(For example, could a system be designed where consumers' protections and permissions travel with their data to protect against misuse or unauthorized disclosure?)

As we've stated, these technologies, standards, and models to a large extent exist, but political process may be inhibiting their adoption. In terms of models or standards, we are proponents of creating a privacy infrastructure that:

- Relies on peer-to-peer networks, but supports aggregation of authorized data
- Empowers a consumer with an opt-in permission capability
- Creates an assured privacy layer using proxy technology and a sound PKI strategy

5. Given the limitations that exist in terms of bandwidth and computing power in the wireless area, is it possible to have strong security and privacy without compromising ease of use and speed? What kinds of trade-offs will consumers need to make between convenience and protection?

We believe the limitations cited are not a good excuse for the choices made in specifications like WTLS. Lengthening keys by a few bytes would not seriously impact performance, especially in the newer phones and PDAs. Properly implementing better algorithms could, in some cases, make the protocols more efficient. Choosing better and longer initial vectors without zero padding and transmitting them encrypted would not be as large an overhead problem as suggested (it's the same amount of data in most cases). Using ECDSA would add authentication and prevent eavesdropping and truncation attacks. We believe the newer processors can easily handle these things.

It remains to be seen if the next version of the specifications incorporates better algorithms like SHA-1 and ECDSA, longer key lengths, and protocol improvements such as encrypting alert messages. And it remains to be seen when and how the manufacturers will incorporate faster CPUs. There are business case arguments that consumers will not pay extra for these security features, but with the rise of public concern over privacy and security this may change as well. Having said this we still believe it is possible today to have strong security and privacy without compromising speed and ease of use. Compute power/price ratio is continually improving. If existing technologies are re-evaluated to employ solutions to some of the pressing problems cited *supra*, then the industry can achieve better levels of privacy and security. However, there are consumer tradeoffs. The two most significant are:

- **Price/Performance.** Security technologies require more on-board hardware capability, which can

raise costs. Accordingly, the “security-enabled” wireless device will generally cost more than the unprotected device. And until there is either regulation or a terrible catastrophe (e.g., identity theft that gains national or congressional attention), consumers will not spend the required time, energy, or thought processes to make the “right” decision, and the unprotected devices will win out.

- **Style/Performance.** Small is in, and getting smaller by the month. With a reduced footprint for hardware, security feature/functions may be the first to trade-out. In the rush to get the smallest, flashiest device, consumers will have to make a personal information tradeoff. Unfortunately, similar to home security systems, until a loss is sustained, consumers won’t spend the time, money, or thought processes evaluating this tradeoff. The result is that product manufacturers will not be driven to incorporate higher grades of privacy or security until a business case can be established, and the business case won’t be established until there is market demand. Market demand, as noted will require consumers understanding or experiencing a clear and present need.

6. Are there limits to the amount of privacy and security protection that can be achieved technologically? If so, what are the other elements needed to ensure consumers’ privacy?

For example, what might be the role of self-regulation, government regulation, market forces, civil law/liability, or employee training?

Yes, and we believe there are four elements that must be addressed to better assure consumer privacy.

1. **Key Management** – People will forget their keys or give them away.
2. **Education** – Unless consumers understand the risk to their personal well being in an unsecured transaction mechanism such as the ones being deployed today in the wireless space, price and style will always win out.
3. **Regulation** – While we believe that market forces will be sufficient industry motivators, we also believe there is an important role for reasonable and appropriate government partnership and initiative through prudent legislative and regulatory guidelines.
4. **Incentives** – MEconomy is founded on the belief that unless the incentives of the advertisers, the marketers, and the consumers are aligned, these privacy and security concerns will continue. Consumers have to be motivated to care about the control over their personal information. Advertisers have to be motivated to care about not compromising consumers’ personal information. Marketers have to be motivated to not gather and misuse information. A system like MEconomy’s assured privacy layer rewards consumers for authorizing specific uses of their data – giving permission to destinations and other Web services to leverage their data on a sliding scale of rewards, incentives, and other benefits. At the same time, this same system must (and will) provide a layer of assured privacy.