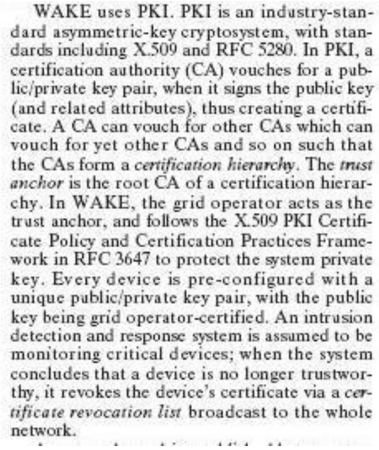
Pervasive Monitoring technology development must consider the unintended consequences of deployment and implementation of X.509v3 devices. Any specification or architecture must include ethical considerations and associated vulnerability and threat scenarios. Only by doing so will the industry recognize its responsibility Vis-a-vie consumer risk. An example of misguided intention follows:

"The ZigBee[1] Alliance [23] is "an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard". It counts 400+ member companies across all worlds that collaborate to define a set of technical specifications for a large set of applications based on low-power wireless communication technology. Thanks to its worldwide adoption, ZigBee specifications often become de-facto standards adopted by the majority of industries. In some cases, ZigBee also liaise with official de-jure standardization bodies in order to improve acceptance and value of its achievements."

Note, no mention of associated ethics, vulnerabilities or threats and their impact on the consumer in this string of adjectives, i.e., after the word *enable*. Who is going to assess these elements? In an asymmetric world the consumer hasn't the knowledge to neither understand nor recognize when they are impacted by pervasive monitoring technology. If the technologist doesn't consider these things no one will, and our economy is placed at risk either due to consumer rejection or worse pervasive attack by an outside criminal element. The only mention of risk in the document occurs, page 100, talking about trading operations.

Another example from RFC 5280 and the IETF[2], *"As privacy has become increasingly important, the Internet Architecture Board (IAB) developed guidance for handling privacy considerations in protocol specifications, and documented that in RFC 6973. And there are ongoing developments in security and privacy happening within the IETF all the time, for example work has just started on version 1.3 of the Transport Layer Security (TLS, RFC 5246) protocol which aims to provide better confidentiality during the early phases of the cryptographic handshake that underlies much secure Internet traffic."* Note that in the specification discussion on WAKE below, IEEE Communications Magazine, January



WAKE uses PKI. PKI is an industry-standard asymmetric-key cryptosystem, with standards including X.509 and RFC 5280. In PKI, a certification authority (CA) vouches for a public/private key pair, when it signs the public key (and related attributes), thus creating a certificate. A CA can vouch for other CAs which can vouch for yet other CAs and so on such that the CAs form a *certification hierarchy*. The *trust anchor* is the root CA of a certification hierarchy. In WAKE, the grid operator acts as the trust anchor, and follows the X.509 PKI Certificate Policy and Certification Practices Framework in RFC 3647 to protect the system private key. Every device is pre-configured with a unique public/private key pair, with the public key being grid operator-certified. An intrusion detection and response system is assumed to be monitoring critical devices; when the system concludes that a device is no longer trustworthy, it revokes the device's certificate via a *certificate revocation list* broadcast to the whole network.

[1] http://www.fi-ppp-finseny.eu/wp-content/uploads/2013/04/D6.3_Electronic-Marketplace-for-Energy-Functional-Architecture_v1.0.pdf

[2] http://www.ietf.org/blog/2013/09/security-and-pervasive-monitoring/

2013, Vol 51, No 1, Page 37, we see a dependency on PKI and certification authority. It is imperative that we recognize that without significant effort placed on security the impact on data privacy, data integrity and confidentiality is considerable. So consensus in and of itself doesn't imply mitigation of consumer risk due to vulnerability and threat from an outside or inside criminal element. Nor does it ensure an ethical treatment of the consumer.

I believe ethical principles must be included in our efforts to design a new world leveraging Internet ubiquity and ease of use. One example of a failure to assess implication of our hubris is Stuxnet[3], it targeted SCADA systems in general. Hence, it is possible that first-strike belongs to the nation with the best decryption capability, e.g., bring on quantum computing. The question I raise is this: USCC cyber technology promotes first-strike capability thereby undermining SALT II and NPT Treaty? It also impacts the OECD Guidelines on Privacy protection and Trans-boarder Flows or Personal Data, and it would undercut or interdict any tool that relied on Pervasive Monitoring.

The ethical principles I am most concerned about are those that affect the consumer specifically in the area of healthcare delivery. I believe that the implementation of HER, HIE, Cloud, CPOE, and any future techno logy leveraging Internet capability is at risk. Hence, technologists working on standards, architectures and tools, must consider the following:

- Informed consent, i.e., the patient once given an opportunity to > assess and concur with the potential for information loss, use, destruction or manipulation brought about through the use of 360X-compliant technologies could exercise informed consent. Patients' right of self-decision can be effectively exercised only if they possess enough information to clearly comprehend their choices and this choice is enabled through the technology.>

- Confidentiality, i.e., the patient's confidential relationship with their referring physician, i.e., a trust relationship, and subsequent clinicians, will not guarantee the integrity of their PHI because the information they reveal to one healthcare provider in private has limits on how and when it can be disclosed to a third party. Thus, physicians or the implementation could advise patients that their PHI could be viewed by third parties without their consent. Given this truth, a patient centric technology is more useful if patients had the ability to provide instructions regarding the distribution and use of their PHI.

- Double-effect, i.e., whenever a physician advises their patient that bad affects, including adverse events, could occur due to the corruption, misuse, or loss of their PHI, it enhances the trust relationship and ensures awareness of potential risk when this advice is integral to 360X closed loop referral workflow. I believe that VP Cheney had a pace maker installed, and his physician demanded that the vendor turn off the wireless network feature. Why, because it could have been hacked and the VP could have been killed with a cyber initiated electronic shock, i.e., if the pace maker were programmed incorrectly, e.g., by a hacker or cyber terrorist.

[3] http://en.wikipedia.org/wiki/Stuxnet

- Beneficence and non-maleficence, i.e., We perceive that the benefits of implementing DIRECT and 360X methods for closed loop referrals far outweigh the potential for harm, such that, even if the information patients provide are misused, the patient is still protected with checks and balances in the technology that are self-correcting.

In conclusion, all technologists have a responsibility to the citizen to ensure privacy and security of information and to include ethical principles in any design, specification, architecture or tool. The asymmetric world we live in demands a more thorough approach. Please consider having this discussion on this important aspect of design.