# A ‘VALUES’ FRAMEWORK FOR DESIGNING INTERNET OF THINGS APPLICATIONS

**Nancy L Russo**
*Internet of Things and People Research Center, Malmö University, Malmö, Sweden*
Email: nancy.russo@mah.se

**Abstract**

*The Internet of Things phenomena is reflected in the increase in the types of devices that can be joined to form computing ecosystems, the growth of the amount and variety of data collected and processed, and the power and reach of applications that can be created on these platforms. While these new applications provide potentially valuable new capabilities to individuals, organizations, and society, they also entail significant risks. This paper presents the VALUES framework to identify potential impacts that should be addressed when designing Internet of Things (IoT) applications. For each of the six areas, questions and issues that should be considered are discussed.*

**Keywords**: Internet of Things, Quantified Self, Personal Informatics

## 1.0 Internet of Things Applications

The Internet of Things refers to “objects that are readable, recognizable, locatable, addressable, and controllable via the Internet – whether via RFID, wireless LAN, wide-area network, or other means” (National Intelligence Council, 2008). Technologies such as near-field communications, real-time localization, and embedded sensors turn “everyday object into smarts objects that can understand and react to their environment” (Kortuem et al., 2010, p. 30). This implies that almost any object, from a thermostat to a running shoe, can become part of the Internet of Things. As early as 2008 it was estimated that the number of devices on the Internet exceeded the number of people on the Internet, and the number of connected devices is expected to reach 50 billion by 2020 (Swan, 2012). The true power of IoT comes not simply from the number of devices but from the ability to combine vast quantities of data from several heterogeneous sources and share that data with other systems (Kranz et al., 2010).

Today there are three main market segments where there is significant IoT activity: smart homes and buildings, transportation, and personal health tracking (Atzori, 2010; Swan, 2012). In homes and buildings sensors, thermostats, and heating and cooling systems are connected with applications to manage energy usage based on occupancy patterns. Trucks, trains, and airplanes may contain components that monitor usage levels and behaviors to determine when maintenance is needed, and communicate that information to both the operator and the manufacturer. "One of the biggest IoT growth areas is measuring individual health metrics through self-tracking gadgets, clinical remote monitoring, wearable sensor patches, Wi-Fi scales, and a myriad of other biosensing applications" (Swan, 2012, p. 218). This is exemplified by the Quantified Self movement, wherein individuals record and track numerous types of data about themselves over time.

In the workplace, IoT technologies were initially used in a manner analogous to their use in smart homes, controlling lighting, heating and cooling and monitoring energy usage. Location-based sensors, including RFID, used to track the movements of employees, have been integrated with these lighting, heating and cooling controls. IoT technologies are being tested for use in training (McGowan, 2015), injury prevention (Kortuem et al., 2010), promoting cohesion (Kirkham et al., 2013), space utilization and employee interactions (Mathur et al., 2015) and security and surveillance (Miorandi et al., 2012), as well as the monitoring of employee fitness and stress levels (Mirarchi et al., 2015; Nield, 2014). "The potential economic benefits to an organization such as reduced absenteeism, increased productivity, increased stress tolerance and improved decision-making, as well as the physical and mental health benefits for employees, means that there is a strong business case for using the workplace as a vehicle for health promotion efforts of this kind" (Kreis & Brodeker, 2004, as cited in McEachan, et al., 2011, p.1)

## 2.0 Designing IoT Systems of the Future: The VALUES Framework

Our understanding of IoT systems design, application, and use is in its infancy. Early work has focused on creating platforms, standards, and devices. Little work has been done to provide guidance on how IoT application systems should be designed to address the risks inherent in these systems and the conflicting needs of different user groups such as individuals and their employers, for example. A preliminary set of issues that may be used to guide designers of IoT application systems to consider issues beyond the functional specifications of such systems, termed the 'VALUES' framework, has been developed from an examination of extant IoT research. Concerns related to each of these issues are briefly described below.

### 2.1 Visibility

We know that relevant data should be presented to users in a simple, intuitive, actionable format (Mathur, et al., 2015). However, these characteristics may not be simple to discern in practice, and the desirable levels may differ between individuals and over time, requiring user customization or co-creation of output (Kirkham et al., 2013). The timescale over which data is displayed may determine whether or not the data has actionable meaning, and correlation with other data may be needed to enable meaningfulness (Swan, 2012). Issues to consider when designing visualizations of data include:

- What data is visible to the individual and to others, and in what format on what platform?
- Granularity: Is data identified/reported at the individual, group, or organizational level, or controlled by the context (Kortuem et al., 2010), and over what timescale?
- Is the data visible to other systems or to external users?

### 2.2 Autonomy

Individuals want to have some control over what data is captured and when and what is done with that data. From the user perspective, active monitoring systems in which individuals enter data themselves or opt-in to data collection provide more autonomy than passive systems which collect data about people without their interaction (Jeske & Santuzzi, 2015). From the system perspective, individuals prefer to have IoT systems running either unobtrusively in the background, when appropriate, or to have complete transparency and control (Kirkham et al., 2013). The level of autonomy may be seen as ranging from totally in the control of the IoT computing system (ambient), or shared between humans and IoT agents either as cooperation between independent agents or as an augmentation of human abilities (Ohlin and Olsson, 2015).

- Which functions should be performed by the system independently and in the background and how should users be made aware of this?
- How much control do users have over data collection and use?
- How can trust between agents be achieved and maintained?

### 2.3 Localization

The context of an individual's movements may be used to determine what data to track or what information to provide (Kortuem et al., 2010). Whereas it is possible to use GPS to continuously track an individual's location, that level of detail may not be appropriate or necessary.

- Does tracking stop at the end of the workday?
- Are relationships between individuals' location data correlated?
- Is location data combined with other types of data?

### 2.4 Utilization

Whereas we might expect the projected use of the data to be a primary driver of system design, in IoT systems data is often collected simply because it can be collected, with the assumption that it might be used in the future. Data from IoT systems may be used for self-monitoring, where an individual can track her own activity and mood, or can serve as a basis for gamification to encourage desired actions (either by the individual or an organization) or can be used for performance evaluation or control purposes by an employer organization.

- What is the purpose and who benefits? Using data for employee development purposes versus performance evaluation reduces negative reactions to monitoring (Jeske & Santuzzi, 2015).
- Are uses legal and/or ethical?
- Who determines how data can be used (including data ownership and control)?

### 2.5 Engagement

The use of many IoT applications is voluntary, determined by the individual user. To achieve the ultimate goal of many of these systems (personal or organizational), users must continue to use these systems in the prescribed manner over the long term. However, in practice there has been a lack of sustainable usage of IoT devices (Swan, 2012). The key to achieving long-term use is to engage the users is such a way that they find on-going value and/or enjoyment in the use of the system.

- What methods of coaching are useful and appropriate?
- What data is needed to allow personalized recommendations?
- What incentives work in which contexts, for which users?

### 2.6 Security

Very often the data captured by IoT systems are personally identifiable, raising issues of authentication, data integrity, and privacy (Atzori et al., 2010). Data may be stored on many different devices in the ecosystem, and for indefinite periods of time, both of which increase the danger of unauthorized access.

- How is distributed data collection and storage documented and monitored?
- In a multi-agent ecosystem, who is responsible for data security at each access point?
- Who creates and implements data access rules?

## 3.0 Conclusion

The IoT issues identified above have implications for individuals, organizations, and society. These issues are not intended to be a comprehensive set of design decisions, but instead serve as a starting point for considerations that should be addressed beyond the functional specifications of IoT systems design. We can expect IoT systems to become more pervasive and connected, and it therefore is in our best interest to establish guidelines, policies and standards to protect the rights of individuals while allowing organizations and society to benefit from the opportunities provided by these systems.

## Acknowledgements

This work was partially financed by the Knowledge Foundation through the Internet of Things and People research profile.

## References

Atzori, L., Iera, A., and Morabito, G. (2010) *The internet of things: a survey*, Computer Networks, 54 2787-2805.

Jeske, D. and Santuzzi, A.M. (2015) *Monitoring what and how: psychological implications of electronic performance monitoring*, New Technology, Work and Employment, 30 62-78.

Kirkham, R., Mellor, S., Green, D., Lin, J. S., Ladha, K., Ladha, C., Jackson, D., Olivier, P., Wright, P. and Ploetz, T. (2013) *The break-time barometer: an exploratory system for workplace break-time social awareness*, In Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, ACM, pp. 73-82.

Kortuem, G., Kawsar, F., Fitton, D., and Sundramoorthy, V. (2010) *Smart objects as building blocks for the internet of things*, Internet Computing, 14 44-51.

Kranz, M., Roalter, L., and Michahelles, F. (2010) *Things that twitter: social networks and the internet of things*, In What can the Internet of Things do for the Citizen (CIoT) Workshop at The Eighth International Conference on Pervasive Computing, pp. 1-10.

Kreis, J. and Bodeker, W. (2004) *Health-related and economic benefits of workplace health promotion and prevention: summary of the scientific evidence*, BKK Bundesverband; Hauptverband der gewerblichen Berufsgenossenschaften - HVBG; Berufsgenossenschaftliches Institut Arebeit und Gesundheit - BGAG.

Mathur, A., Van den Broeck, M., Vanderhulst, G., Mashhadi, A., and Kawsar, F. (2015) *Tiny habits in the giant enterprise: understanding the dynamics of a quantified workplace*, In Proceedings of the 2015 ACM Int'l Joint Conf. on Pervasive and Ubiquitous Computing, pp. 577-588.

McEachan, R. R., Lawton, R. J., Jackson, C., Conner, M., Meads, D. M., and West, R. M. (2011) *Testing a workplace physical activity intervention: a cluster randomized controlled trial*, Int J Behav Nutr Phys Act, 8 1-12.

McGowan, M. (2015). *One Eye on the Future: NIU professors harness an empowering potential of Google Glass*. Available at: http://newsroom.niu.edu/2015/10/08/one-eye-on-the-future/ (accessed 8 October 2015).

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012) *Internet of things: vision, applications and research challenges*, Ad Hoc Networks, 10 1497-1516.

Mirarchi, D., Vizza, P., Cannataro, M., Guzzi, P. H., Tradigo, G., and Veltri, P. (2015, June). *ICT Solutions for Health Education Model*, In Computer-Based Medical Systems (CBMS), 2015 IEEE 28th International Symposium, IEEE, pp. 31-32.

National Intelligence Council (2008) *Disruptive Technologies Global Trends 2025: Six Technologies with Potential Impacts on US Interests out to 2025*, Available at: http://www.fas.org.irp/nic/disruptive.pdf (accessed 12 October 2015).

Nield, D (2014) *In corporate wellness programs, wearables take a step forward* Fortune.com. Available at: http://fortune.com/2014/04/15/in-corporate-wellness-programs-wearables-take-a-step-forward/ (accessed 8 August 2015).

Ohlin, F. and Olsson, C.M. (2015) *Intelligent computing in personal informatics: key design considerations*. In Proceedings of IUI 2015, ACM, Atlanta, USA, pp. 263-274.

Swan, M. (2012) *Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0*, Journal of Sensor and Actuator Networks, 1 217-253.