Digital Data and the City

An exploration of the building blocks of a Smart City Architecture

J.H. van de Pas, . G.J. van Bussel, . M. Veenstra, F, Jorna

Introduction

According to technology pundits, we are at the brink of an information (technology) revolution. Within a decade, the "Internet of Things" (IoT, the interconnection of uniquely identifiable devices within the Internet infrastructure (Holler, et al., 2014), will generate huge amounts of digital data. This data may be applied to manage the urban environments in which the majority of the population of the world is living. Those urban environments will be turned into 'smart cities'. The subject of the smart city is discussed extensively within scientific and political communities. Most attention is paid to the new and exciting possibilities that integrated information technology systems (ICTs) have to offer to citizens of these smart cities (Townsend, 2013). What is less discussed is the process of information management (IM) that is instrumental to the application of the ICTs within a smart city. The huge amounts of data necessary to manage a smart city require IM models that match the unprecedented scale of data processing that is required. This is highly relevant, because it is acknowledged in literature that the societal impact of this scale of data processing cannot be predicted (Mayer-Schönberger, Cukier, 2013). Proper attention to the IM issues that will emerge as smart cities are implemented is therefore highly relevant.

In this chapter we will be exploring smart cities: those cities that succeed in the application of ICTs at a practical level and harvest the benefits of the IoT. We will discuss the application of ICTs and look at the aspects of digital data that are relevant in the 'information value chain' (IVC) that is being executed. We will follow the flow of data from the initial cue that starts the process, as picked up by sensors, the interfaces that provide interaction between the city and the individual citizen, and the intelligence behind the screens that is responsible for the delivery of applicable information to the citizen. We will start with a short sketch of ideas and ideals that underlie the smart city; followed by discussion of building blocks - sensors, screens and actuators - that enable the city environment to interact with the citizen on the street. After that, we delve into the IVC, following the path data takes along that chain in the course of its value creation for the city.

Dreaming of Smart Cities

Anthony Townsend (2013) explores a wide array of technological solutions to different problems cities face today. In his opinion smart cities are 'places where information technology is combined with infrastructure, architecture, everyday objects, and even our bodies to address social, economic, and environmental problems'. Smart cities look very much like the cities we are living in today, but they are able to deliver services to citizens faster, more effectively and in a personalised manner through the application of ubiquitous computing. Townsend (2013) has interviewed countless experts on this subject, and explains how ICTs will make cities ecologically viable, by enabling detailed management of energy, water, traffic, and waste disposal. Crime and vandalism will be prevented by influencing the environment, and steering individuals towards safety or away from trouble. There are developments that directly influence the mood of the people on the streets by light, images and even odour. In order for cities to be able to do this, the 'dumb' built environment (bricks and mortar) has to be augmented by IoT-interfaces, realising a massive application of ICTs that collect large amounts of data that can be processed, analysed, disseminated and used (via IM processes) to influence the urban environment and the city's inhabitants. Compliance to laws and regulations (especially concerning privacy and security) has gained little attention, but it is one of the most essential aspects of smart cities. Smart city governance and compliance architecture is at this time largely undefined (Paskaleva, 2009). Schematically outlined, the *smart* city might be represented as in Figure 1, consisting of four layers (or conceptual containers): Legal Architecture, IM, Interfaces, and Citizens. Interpreting these layers as conceptual 'containers' makes it possible to discern different environments. In reality, the four layers are inherently interwoven and very difficult to discern. We will point out how both 'middle layers – IM and Interface – interact with each other in the Smart City environment. As will be shown, there is more than a marginal difference between the 'classical' IM challenges, that are restricted to a single organisation, or a number of organisations in the case of connected process management, and the ubiquitous computing environment that the smart city brings to life.

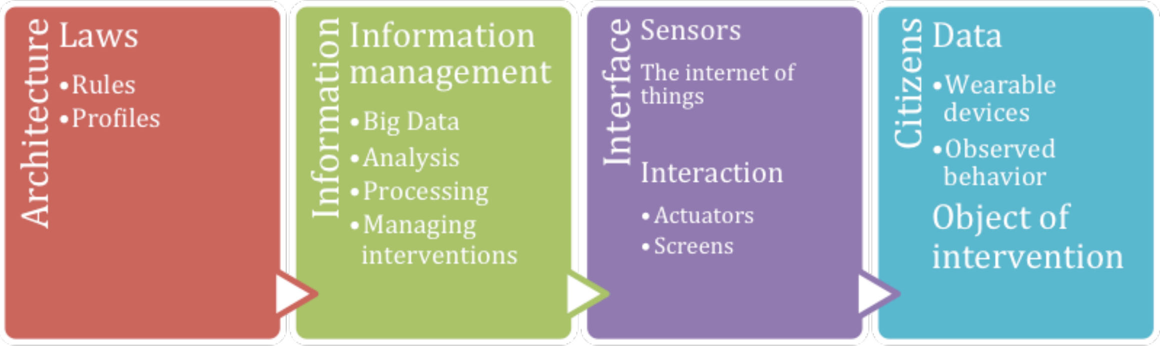


Figure 1. The four layers of a smart city (drawn by JP)

Utopia is becoming reality

In several cities around the world, interfaces (like sensor systems) have been installed and implemented that continuously monitor urban environments and collect enormous amounts of data. ICTs process this real-time data immediately. A smart city is keeping an eye out for all occupants of the streets, people and objects alike. 24 hours a day, 7 days a week, all year long. Monitoring people in the city's public spaces and in their homes as well as gathering, analysing and using data from (local) websites, social media, smart phones, messaging services, weblogs, and so on., does not, however, qualify a city as a truly 'smart' city. For that, the city itself needs to be interactive, to interact with its citizens. ICTs for interactivity, like public screens and actuators, will have to be applied to the built environment, to inform, influence, or even steer citizens in the desired directions. Such (and other, more direct) interventions make it possible to influence the behaviour of citizens. But it is also the other way around: the central technical components of the smart city allow citizens at the same time to exchange data with it, enabling them to influence the city, enjoy useful (personalised) services and to monitor the status of (aspects of) the city.

Townsend (2013) describes smart cities as intelligent entities that

> can adapt on the fly, by pulling readings from vast arrays of sensors, feeding that data into software that can see the big picture, and taking action.... Sometimes, these interventions on our behalf will go unnoticed by humans, behind the scenes within the wires and walls of the city. But at other times, they'll get right in our face, to help us solve our shared problems by urging each of us to make choices for the greater good of all

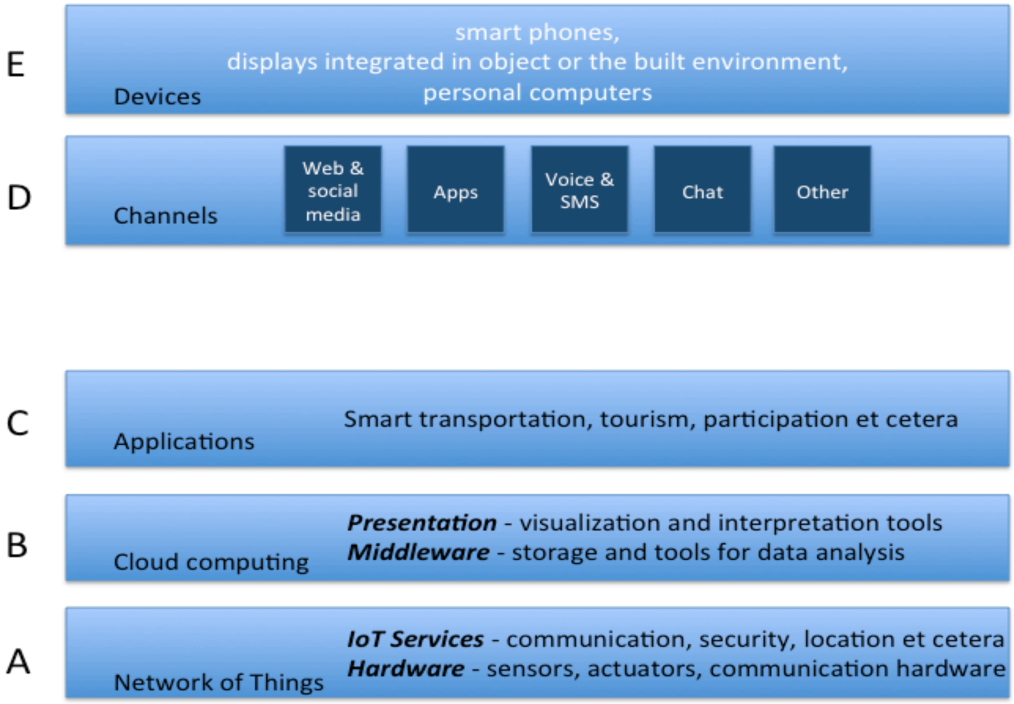
To make this into a reality, the smart city needs to know its occupants intimately. Using data analysis on the endless amounts of data harvested by countless sensors and the personal data from all different kinds of public (and private) sources, the city can provide each and every citizen with the services that each specific citizen is entitled to. Based upon the citizen profiles - the smart city keeps files of all of its citizens - access to or denial of services is determined on an individual basis. Screens and actuators that riddle the city act as ushers, openly or covertly nudging the citizen by sending signals, opening or closing gates, granting or denying access on an individual basis.

It looks like the smart city is becoming the physical manifestation of the concept of 'choice architecture', an architecture that seeks to affect outcomes through the manner in which the person or organisation presents choices to decision-makers (Thaler and Sunstein 2009). Although the starting point of the analysis of Thaler and Sunstein is (applied) psychology, their manifesto breathes a thouroughly rationalised view on life. The smart city may bring the physical manifestation of those behavioural sciences to our streets.

Building blocks of the smart city

Without relatively new ICT phenomena such as big data, IoT, semantic technologies and cloud computing, smart cities will not reach their full potential (Komninos, 2014; Vermesan and Friess, 2014). It is, however, essential to realize that these ICTs are a means to an end. They should not be the starting point or the main perspective when developing a smart city strategy. What should be central in such a strategy is the citizen, more specifically: the value and possibilities that will be created for the daily lives of the citizens of smart cities. Smart cities are complex, fast growing, distributed environments that develop and constitute dense nodal information networks between its governments, citizens and private enterprises to cope with the city's challenges. ICTs in smart cities should be aimed at enabling and stimulating citizens and companies to use, contribute to and shape the city (UN eGovernance Survey, 2014). Despite the fact that building the smart city is a shared effort, governments are responsible for creating the preconditions for smart cities. They have a system-responsibility for the 'wiring' of cities, the integrity of data-storage, privacy, transparency, ICT security, protecting citizens' interests, and level playing fields (Dunleavy et al., 2006). There are a multitude of smart city ICT architecture initiatives in which governmental and municipal organisations are involved (Kartman et al, 2011).

Smart cities are sustainable, inclusive cities where technology enables citizens to enhance their quality of life. They have a multitude of application areas. ICTs will have to be aimed at enabling and stimulating citizens (and companies) to use and shape technology and put it to work. There are three main technological components that enable seamless smart city applications: hardware, middleware and presentation (Gubbi et al., 2013). The hardware component consists of sensors, actuators and embedded communication hardware. The middleware component contains storage and computing tools for data analytics. Finally, the presentation component contains data visualisation and interpretation tools. Hardware is part of the 'Network of Things' (A in Figure 2),


E
Devices
smart phones,
displays integrated in object or the built environment,
personal computers
D
Channels
Web & social media
Apps
Voice & SMS
Chat
Other
C
Applications
Smart transportation, tourism, participation et cetera
B
Cloud computing
Presentation - visualization and interpretation tools
Middleware - storage and tools for data analysis
A
Network of Things
IoT Services - communication, security, location et cetera
Hardware - sensors, actuators, communication hardware

while middleware and presentation are part of 'cloud computing' (B in Figure 2).

On a more detailed level, ten functional building blocks for smart environments are distinguished (McCullough, 2005; Veenstra, 2013). These building blocks are part of the three main technological components that enable smart city applications and of the channels (such as apps and social media, level D in Figure 2) and devices (such as smart phones and displays integrated in the built environment, level E in Figure 2) that make the smart city visible for the people, citizens and professionals. These ten functional building blocks are the following. We start with microprocessors (1, level B) that make it possible that environments and objects can be enriched with computing power. Sensors (2, level A) make it possible for an intelligent environment to perceive changes, for instance a movement or a rise of somebody's blood pressure. The detection of changes makes it possible for smart cities to act. For sensors to act that way, they have to be part of a connected network of devices. There have to be communication links (3, level A). To identify persons and objects in smart cities, tags (4, level A), such as RFID-tags, QR-codes or smart phones with NFC, are necessary. Actuators (5, level A) react upon a change in the environment, for instance the presence of a person or a change in temperature, with a response such as opening a door, showing information on a screen, or manipulating a valve of a (heating) system. Although smart environments could be fully autonomous, controls (6, levels D and E) leave users the possibility to operate the system manually in case of emergency. To inform people or to visualise interaction possibilities, displays (7, level E) are indispensable. To establish the position of a person or an object, positioning technology (8, level A), such as GPS, is an absolute necessity. Intelligent environments can react not only upon data from one specific sensor but also upon something more complex: a situation. Situation Identification (9, level B) can arrange that, combining sensor data with knowledge of the world. Tuning (10, level A) arranges for the incremental adaptation of configurations and settings. Tuning enables meaningful interaction between the components of a smart environment.

Several building blocks of the smart city directly enable or stimulate citizens and professionals to be involved in the smart city. The exchange of data is made possible by these functional building blocks such as tags that identify citizen, sensors that collect data about citizens, actuators that react to citizens or give them feedback, control mechanisms that give them the possibility to influence the system in a more direct way, screens that for instance can convey information and make interaction possibilities visible and positioning systems to determine the position of a citizen. This constitutes the interface to the smart city for its central target group: the people using the city. For a well-functioning smart city sufficient attention to the elements of this interface and the digital data that is exchanged with it is indispensable.

Information Management: Protecting Data 'With Your Life'

Underneath these basic functional building blocks a platform is needed that makes it possible to store, process and retrieve the data collected via, for instance, sensors, controls and positioning systems. The smart city is an increasingly data rich and data dependent platform on which staggering amounts of data are collected, created and used in real time. These enormous quantities of data, Big Data, require special consideration because of their volume, variety, velocity, value, and veracity (Gordon, 2013; Madden, 2012). These data are easily and (mostly) automatically recorded, stored to be accessed, retrieved, and analysed. This analysis creates nearly limitless possibilities, but it might become a liability when the collection, recording and use of data about (or concerned with) citizens happens (as it is most often) without their knowledge or consent. Most of this behaviour takes place behind the scenes, is barely noticed by users, and is done with only our tacit consent. The ease of access to this data in 'the cloud' (on a third party device remotely located from the user) makes a user's relationship with his or her data more tenuous. If this data is hacked, sold, or publicised, it could be a serious breach of privacy (Stylianou, 2010; Van der Pas, Van Bussel 2014). The public-private co-operations within smart cities need to understand their ultimate responsibility for proper protection of this data (Sullins, 2014).

Smart Cities are an exponent of a changing world. They are developing into virtual, interactive, and hyper-connected platforms. As users of mobile, wirelessly interconnected devices, citizens of a smart city are using web-based communities and social-networking sites within the city as new channels for socialising, sharing with friends and colleagues, collaborating, interacting, and participating in professional processes of innovation, production, governance, and creating value. Smartphones are continuously cataloguing and quantifying actions and accessing, creating, and sharing data that can enable faster decisions. Companies and smart city services are building online service stations, shops, communities, user groups, and other ways to promote and deliver their products and services. They are analysing and using the data they are gathering from their citizens, customers and other users of their online services (via websites, social media, sensors, actuators, tags, positioning systems and so forth) to personalise their interactions with them. Libraries, archives and other repositories are digitising their collections and are making them accessible to every user on the smart city platform. Local television has broken out of the living room, onto mobile devices, multiple screens, and on demand. News is broadcasted on Twitter, local news sites and interactive spaces and screens. The smart city is using the semantic web to allow applications and devices to understand the meaning of natural language and to communicate without human interference (Davies,et al., 2002). The IoT is evolving fast, enabled by the development of (wireless) networks without human or centralised components. The IoT includes everything from power and energy meters that report usage data automatically, to wearable heart monitors that send health data to a doctor, and to traffic sensors and cars that will automatically report their position and condition to authorities in the event of an accident.

Data harvesting systems, fed by the upcoming abundance of all kinds of sensory systems that continuously capture data regarding human-environment interaction in the smart city, lead to new challenges in the area of IM, especially for privacy and security. Data, traditionally captured in ICTs by organisations, are breaking loose from the constraints imposed by separate ICTs and are absorbed into a 'cloud'. All data in that 'cloud' are stored, analysed, transmitted and reprocessed in a continuous cycle of IM processes and algorithmic processing. The challenge of facilitating ICTs with proper and fail-proof systems guaranteeing privacy and security during data processing is by no means new (Patnayakuni, Patnayakuni, 2014; Hausmann, et al., 2014). Incidents involving security and privacy infringement are, likewise, not a new phenomenon, especially not in a time of ever more intrusive surveillance technologies and data analysis techniques (Bélanger, Crossler, 2011; Mayer-Schönberger, Cukier, 2013; Van de Pas, Van Bussel, 2014). Privacy infringement is often portrayed as 'natural' to the implementation of ICTs, but organisations developing ICTs make *choices* (Morozov, 2013). Organisations processing data *choose* to add or remove functionalities in their ICTs. That means they may decide to implement, for instance, Privacy Enhancing Technologies (PETs), thereby respecting citizens' privacy during their operations. There is a problem, however. Privacy is a legal concept from the real world, ruled by institutions staffed by people. ICTs are also part of cyberspace, ruled by technology. Each environment comes with its own sets of rules and limitations. Real-world laws may not necessarily apply the same way in global cyberspace. It might well prove more difficult to develop systems that respect privacy law than the catchphrase privacy-by-design promises. The rule of law cannot simply be translated directly within ICTs (Solove, 2004; Lessig, 2006; Van de Pas, Van Bussel, 2014).

Information Management: Information Value Chain

Until a few years ago, IM was deemed a matter of organisations exploiting their own ICTs. Organisations captured their business process data into a digital infrastructure, which did not cross the borders of the organisational structure. They controlled the data that was collected and retained within their ICTs. If privacy, security, or other business related issues arose, a single point of interaction could be contacted by a citizen or privacy authority (Davenport, 1997). That 'point of control' became diffused with [1] the ongoing integration of processes between different organisations, stimulated by the sharing of data through (for instance) social media (McAfee, 2006), and [2] the breakthrough of supply chain and ERP systems, causing data integration (Srinivasan, Dey, 2014). As it became common practice to share data between different parties, it could become difficult to ascertain which of the integrated process owners was responsible for a breach of privacy (if and when that occurred), a security problem, or the accessibility of data. The implementation of data security procedures in order to protect data integrity and to prevent unauthorised data access is not enough. Data security procedures do not lead to compliance to privacy regulations (Borking, 2010).

IM has become challenging with the emergence (and consequent acceleration) of Big Data (especially data analytics) and cloud computing, especially when protecting privacy and security within business processes (Holler, et al., 2014). Judging by the numerous reports of privacy-related incidents, it proves challenging for traditional ways, methods, and technologies to achieve the expected quality of data, data management, compliance and information governance (Van de Pas, Van Bussel, 2014). New data analysis technologies need to be used to explore structured and unstructured data which at the same time provide additional insight, near real-time business analytics, deep analytics, and low cost, highly scalable storage and analytics platforms (LaValle, et al., 2011). At the same time, the ICT infrastructure is gravitating towards a rent model of cloud usage that has the benefit of elasticity. There is an increasing appetite for cloud-based services and platforms, impacting the model of application development and risking a lock-in. Guaranteeing privacy and security in such a dynamically changing ICT environment is an enormous IM problem. To cope with that problem all data and all ICTs need to be identified and controlled (Van de Pas, Van Bussel, 2014).

IM organizes the Information Value Chain (IVC) to identify, control, and manage data and ICTs in and between organisations. This chain ensures that the informational and evidential value of (big) data is utilised in and between business processes to improve performance, privacy, and security by safeguarding the four dimensions of information: quality, context, relevance, and survival (Van Bussel, Ector, 2009; Van Bussel, 2012a; Van Bussel, 2012b). The IVC is a business process model that includes all IM processes within the data flow: generation or receipt, identify, capture, storage, processing, distribution, structuring, publication, (re-) use, appraisal, selection, disposal, retention, security, auditing and preservation. The IVC (see Figure 3) is instrumental in [1] providing proper control on the performance of business processes, [2] providing trusted information, [3] the realisation of the governance and compliance efforts of organisations, [4] providing legal readiness, and [5] the protection of privacy-sensitive data. Security and privacy issues in IM processes must be assessed, using the IVC model, to identify possible risks for the organisation and to take proper actions if breaches of laws and regulations may take place (Haller, 2012). Most organisations, for instance, consider compliance with privacy guidelines primarily relevant at the point where information enters the ICTs of the organisation. That is not completely true. Looking at the IVC model from a perspective of security and privacy risks, infringements appear most explicitly at six points (or IM processes within the IVC), emphasised in Figure 3 as ‘open circles’: generation/receipt of data, processing, (re-)use, appraisal, disposal and preservation.

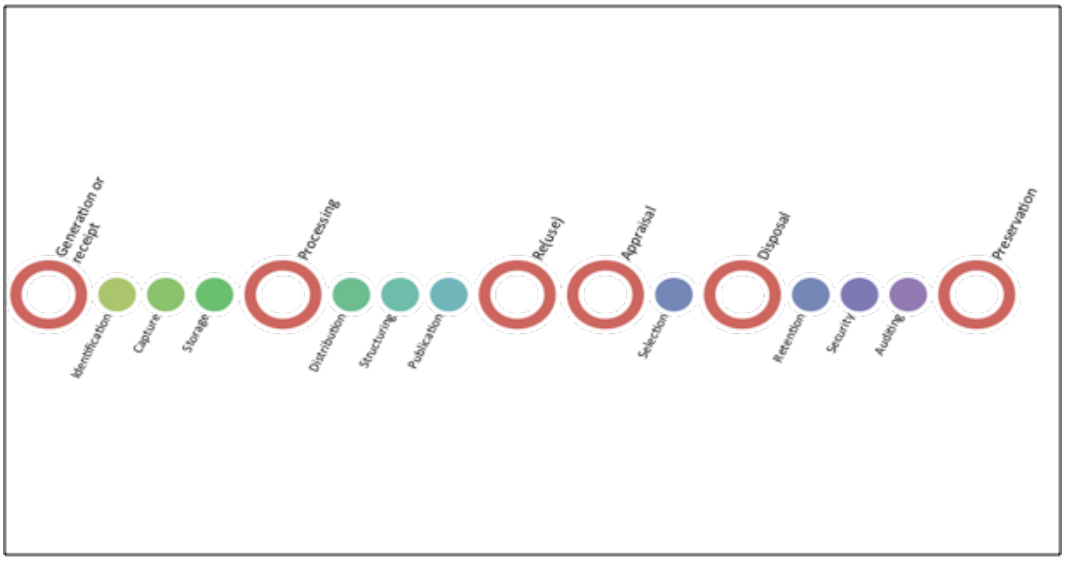


Figure 3. The Information Value Chain according to Van Bussel (2012)

Smart cities need to take proper care of the data they are entrusted with by citizens, because any failure to do so leads to loss of trust, economic value or public support. How to do this properly and who has to take responsibility to make this happen is still open to debate. One thing is for sure: IM is essential for reaching that goal. It should protect data 'with its life'.

A conclusion?

With the emergence of the smart city, local governments want to make cyberspace the primary interface to city architecture. These ambitions may prove to be highly beneficial to cities as a whole and their citizens especially (Barney, 2004). Smart cities emerge in public-private co-operations that may be beneficial, but need checks and balances to address the problem of unchecked power-by-control that ownership of an ICT environment may bring. It takes a lot of effort to design an IM environment to represent the legitimate interest of both the public-private co-operations *and* the citizen at the same time. Laurence Lessig (2006) warns that assumptions that it is possible to control the merger of cyberspace and 'real space' without doing any harm, are untrue. In his view, choices about which values have precedence within ICTs, about regulation, about control, and about privacy and security, are political choices. They need to be 'coded' to be realised. And yet, 'oddly, most people speak as if code were just a question of engineering. Or as if code is best left to the market. Or best left unaddressed by government'.

In our opinion, those choices cannot be left to the market *alone*. They *have* to be addressed by (local) governments. Governments need to accept the mechanisms that underlie the implementation of ICTs. There is no such thing as behaviour in cyberspace without consequences in real-life smart cities. If we really want governance, transparancy, privacy, and security to be realised, the building blocks of a smart city need to be implemented and regulated. Attention to IM in the debate about the smart city is sorely missed. The actual debate until now revolves around services and business models. We believe Information Management should be defined as a new, essential building block of a smart city: it is imperative for implementing, managing, and realizing the Information Value Chain to safeguard the four dimensions of information for all data, datasets and ICTs under its control. We strongly support the assertion of Laurence Lessig (2006): in each smart city public-private co-operation, the choices about the prevalence of values should be made consciously, before being coded into the software and hardware infrastuctures.

Judging by the discussion on smart cities, we are standing at the brink of a new era in human history, possibly comparable to the full-scale breakthrough of the steam engine in the early 1800's. That technological revolution changed production and transportation, and caused massive societal changes. The merger of cyberspace and the built environment in smart cities shows comparable potential. For better or for worse: proper attention to IM in these future cities is a subject that is too important to be ignored.

References

Barney, D. (2004). *The network society* (Cambridge: Polity Press).

Bélanger, F., R.E. Crossler (2011). 'Privacy in the digital age. A review of information privacy research in information systems', *MIS quarterly* 35, no. 4, pp. 1017-1042.

Borking, J. (2010). *Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies* (Deventer: Kluwer)

Davenport, T.H., L. Prusak (1997). *Information ecology: Mastering the information and knowledge environment* (New York: Oxford University Press).

Davies, J., F. van Harmelen, D. Fensel (2002). *Towards the semantic web: ontology-driven knowledge management* (New York: John Wiley & Sons).

Dunleavy, P., H. Margetts, S. Bastow, J. Tinker (2006). *Digital Era Governance. IT coporations, the state and e-government* (New York, Oxford: Oxford University Press, 2006)

Gordon, K. (2013). "What is Big Data?", *ITNOW* 55, no. 3, pp. 12-13.

Gubbi, J., R. Buyya, S. Marusic, M. Palaniswami (2013). 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, 29, no. 7, pp. 1645-1660.

Haller, K. (2012). 'Data-privacy assessments for application landscapes: A methodology', F. Daniel, K. Barkaoui, S. Dustdar (eds.), *Business Process Management Workshops*, 2 (Berlin-Heidelberg: Springer), pp 398-410.

Hausmann, V., S.P. Williams, C.A. Hardy, P. Schubert, 'Enterprise Information Management readiness: A survey of current Issues, challenges and strategy', *Procedia Technology* 16 (2014), pp. 42-51.

Holler, J., V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, D. Boyle (2014). *From machine-to-machine to the Internet of Things. Introduction to a new age of intelligence* (New York: Academic Press)

Kartman, G., A. Sandnes, G. Smit (2011). 'Creating municipal ICT architectures. A reference guide for smart cities'. Online source (Nov. 20, 2014): http://www.smartcities.info/creating-municipal-ict-architectures-reference-guide-smart-cities.

Komninos, N. (2014). *The age of intelligent cities: smart environments and innovation-for-all strategies* (London: Routledge).

LaValle, S., E. Lesser, R. Shockley, M.S. Hopkins, N. Kruschwitz (2011). 'Big data, analytics and the path from insights to value', *MIT Sloan Management Review* , 52, no. 2, pp. 21-31.

Lessig, L. (2006). *Code, and other laws of Cyberspace, version 2.0* (New York: Basic Books).

Madden, S. (2012). "From databases to big data", *IEEE Internet Computing* 16, no. 3. pp. 0004-6.

Mayer-Schönberger, V., K. Cukier (2013). *Big data. A revolution that will transform how we live, work and think* (London: John Murray)

McAfee, A. (2006). 'Enterprise 2.0: the dawn of emergent collaboration', *MIT Sloan Management Review* 47, no. 3, pp 21-28.

McCullough, M. (2004). *Digital Ground. Architecture, pervasive computing, and environmental knowing* (Cambridge: MIT Press).

Morozov, E. (2013). *To save everything, click here. The folly of technical solutionism* (New York: Public Affairs)

Paskaleva, K.A. (2009). "Enabling the smart city: The progress of city e-governance in Europe." *International Journal of Innovation and Regional Development*, vol. 1, no. 4, pp. 405-422.

Patnayakuni, R., N. Patnayakuni, 'Information security in value chains: A governance perspective', *Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS 2014), Association for Information Systems* (Savannah, 2014), pp. 1-10. Online source (Nov. 20, 2014): http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1161&context=amcis2014

Solove, D.J. (2004). *The Digital Person. Technology and privacy in the information age* (New York, London: New York University Press).

Srinivasan, M., A. Dey (2014). "Linking ERP and e-business to a framework of an integrated e-supply chain", F.J. Martínez-López (ed.), *Handbook of Strategic e-Business Management* (Berlin-Heidelberg: Springer), pp 281-305.

Stylianou, K.K. (2010). 'Hasta La Vista privacy, or how technology terminated privacy', C. Akrivopoulou, A. Psygkas (eds.), *Personal data privacy and protection in a surveillance era. Technologies and practices* (Hershey (Pa.): IGI Global, 2010), Ch. 3, pp. 44-57.

Sullins, J. (2014). 'Information technology and moral values', E.N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Stanford: Stanford University). Available online at: http://plato.stanford.edu/archives/spr2014/entries/it-moral-values/ (Online source, Nov 22, 2014).

Thaler , R. H., C.R. Sunstein (2009). *Nudge: improving decisions about health, wealth and happiness* (London: Penguin Books).

Townsend, A. (2013). *Smart Cities. Big Data, civic hackers and the quest for a new utopia.* New York & London: W.W. Norton & Company.

United Nations eGovernment Survey. E-Government for the future we want (New York, United Nations, Department of Economic and Social Affairs, 2014).

Van Bussel, G.J. (2012a). *Archiving should be just like an Apple™ en acht andere, nuttige (?) stellingen* (Amsterdam: Amsterdam University Press.

Van Bussel, G.J. (2012b). 'Reconstructing the past for organizational accountability', *The Electronic Journal of Information Systems Evaluation*, 15, no. 1, pp. 127-137.

Van Bussel, G.J., F.F.M. Ector, *Op zoek naar de herinnering. Verantwoordingssystemen, content-intensieve organisaties en performance* (Helmond: Van Bussel Document Services, 2009).

Van de Pas, G.J. van Bussel (2014). 'Privacy lost - and found ? Some aspects of regaining citizen's privacy by means of PET in the age of Big Data', J. Devos, S. De Haes (eds.), *Proceedings of the 8th European Conference on IS Management and Evaluation. ECIME 2014. University of Ghent, 11-12 september 2014* (ACPI: Reading, 2014), pp. 278-285.

Veenstra, M. (2013). *Informatietechnologie in de openbare ruimte. Bron van mogelijkheden en gevaren* (Amsterdam: Amsterdam University Press).

Vermesan, O. P. Friess (2014). *Internet of Things – From research and innovation to market deployment* (Aalborg: River Publishers).