Georgia Tech | Center for the Development and Application of Internet of Things Technologies

Driving New Modes of IoT-Facilitated Citizen/User Engagement

Envisioning New IoT-Centric Approaches and User Experiences that Enhance Citizen Satisfaction, Participation, and Engagement

July 2018
Atlanta, Georgia, USA

Georgia Institute of Technology (Georgia Tech)
Center for the Development and Application of Internet of Things Technologies (CDAIT)
IoT Thought Leadership Working Group

PREFACE

This White Paper was born out of discussions and exchanges about the nature, direction and challenges of the Internet of Things (IoT) over twenty-four months starting in June 2016 within the IoT Thought Leadership Working Group of the Georgia Institute of Technology (Georgia Tech) Center for the Development and Application of Internet of Things Technologies (CDAIT)[1].

IoT-facilitated user/citizen engagement across the Smart City ecosystem is the "case in point" for the overall report.

The effort was spearheaded by Karen I. Matthews, Ph.D. (Corning), Chair; and Paul M.A. Baker, Ph.D. (Georgia Tech); Clay Mahaffey (Kimberly-Clark); and Forrest Pace (AIG), Vice Chairs; and sub-group leaders Jerome Holbus (Infor), Johnny Parham (Infor), Doug Guthrie (Comcast) and Kelly Arehart (Kimberly-Clark).

The contributors whose names are listed at the end of the paper come from different walks of industry and academia, and are directly involved in the building of IoT. They shared personal ideas, observations and opinions grounded in real-life experience.

As a result, the views expressed in this White Paper are solely the authors' collective own and do not necessarily represent those of Georgia Tech, the CDAIT company members, the individual members of the IoT Thought Leadership Working Group, the University System of Georgia or the State of Georgia.

[1] Information about CDAIT and the CDAIT IoT Thought Leadership Working Group can be found at the end of the White Paper.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

Page intentionally left blank

EXECUTIVE SUMMARY

This White Paper sets out to examine how the Internet of Things is markedly reshaping user engagement, defined here as a stakeholder's response to some type of offering, such as, but not limited to, a product or a service.

It starts with a brief overview of the Internet of Things (IoT) and explores IoT applications with an end-user focus. Through the framework of user engagement within a Smart City, i.e., citizen engagement, it investigates a range of potential IoT applications and challenges for five key Smart City use cases: municipal services management, utilities, public safety, transportation, and healthcare.

We submit that the expression "Internet of Things" should not be taken literally; it is a metaphor that refers to a radical paradigmatic transformation, i.e., the interconnection of intelligent things, which is bound to bring about dramatic economic and social changes.

In the introduction, we highlight the complexity of the IoT value chain, made up of numerous moving parts, and the convergence of timely trends that have contributed to the current global attention on the Internet of Things.

The paper intends to answer four key questions:

1. What are the opportunities for, and limits of, Smart Cities and connected users/communities?
2. What data ownership and security issues are associated with IoT and how will they be addressed?
3. What will IoT business models look like and what would constitute "success"?
4. What possible roadmaps can lead to the IoT revolution becoming the IoT of the future?

IoT should not only be thought of as a collection of technologies, but also include societal impacts and benefits as well as social outcomes that can be advanced, enhanced and simplified by the use of "smart" technologies. Through data capturing, sharing and processing, both the private and public sectors can devise specific, data-driven solutions integrating social, economic, policy and contextual inputs. User feedback will ensure that the solutions are meeting citizen needs.

From a policy perspective, it is imperative that cities also address a variety of stakeholder needs and concerns as projects are being justified and developed. Citizens must receive sufficient information to enable them to develop a clear understanding of how the data is being used, and who has ownership and control of this data. Hence, two key areas that are becoming increasingly important as we move toward connected "things" that utilize smart technologies are security and privacy, two interrelated but separate issues.

While *security* refers to protecting data/information from being improperly accessed and/or affected, *privacy* refers to the right of an individual (or entity) to determine use of data/information, consistent with their preferences.

Both aspects should be addressed "by design" as we move toward data-rich, connected environments with porous or poorly defined boundaries. Due to the nature of many IoT devices (ubiquitous "always on" deployment, limited computing capabilities, limited memory, and extreme power limitations), security can be especially difficult to manage. These limitations complicate on-device security; therefore, security must be holistic, systemic and systematic to ensure data integrity.

Similarly, privacy must be addressed both at the level of the individual user as well as at the system level, with policies and procedures playing a fundamental role in addition to technology.

A connected society will require a higher level of integration of increasingly complex IoT implementation platforms, but a real user-centric IoT system should be making *citizens more aware and truly "smarter"* rather than showcasing technology for technology's sake.

Successful implementations of IoT for communities will closely match citizens' conditions and needs with systems that are convenient. They will also provide straightforward connection to data sources of interest, thus generating a value proposition that is clear and evident.

The *EPIC* analytic approach is introduced to help municipalities (and any other organized collectivity in charge of the public interest that is investigating the potential use of IoT technologies) review the opportunity and impact of investing in IoT. EPIC screens the IoT effort through four variables: Ethics, Profit (economic and social), Intimacy, and Connectivity.

It is critical to evaluate the "goodness of fit" of a business model (or other new monetization method) via the use of trials rather than a "big bang" implementation of what seems to be a good idea but has no measurable evidence of fit. Designing these trials to be representative and scalable will be essential.

Since citizens are the ultimate benefactors of these platforms and their related initiatives, we propose *Design Thinking* as one approach to developing user-centric IoT solutions that will have the maximum community benefit. It incorporates many decades' worth of research across multiple disciplines to create a path to problem solving that puts the end user at the center of the work. Through careful questioning, rapid prototyping, and iteration, the citizen can quickly provide feedback that helps determine whether a solution actually solves the need in the way he/she finds beneficial.

The Internet of Things is in its infancy, and therefore all related activities require prudent and judicious management. If hastily deployed enabling technologies do not deliver on the expected outcomes on both the technological and human axes, cities will not be as enthusiastic in their support. As a result, if not denied, IoT innovation will be delayed.

Leveraging design thinking can at least help mitigate some of this risk. Good design affects not only the 'goodness of fit' of an IoT service to the community but also the service rollout itself. It should be noted that system interdependence calls for a holistic approach mindful of the complexity and interconnectedness inherent to Smart Cities.

By focusing on universal design (i.e., creating products and services everyone can use and that are, ideally, universally compatible), stakeholder involvement, security and privacy by design, economic and social feasibility, and sustainability, Smart Cities' IoT implementations will be successful through fostering meaningful citizen engagement and meeting the needs of all parties involved.

Smart Cities endeavor to tackle the present and future problems by solving pressing issues while still making sound fiscal decisions. This is sometimes slow but always challenging. However, little by little, IoT technology drivers and conditions of necessity within use cases are molding today's IoT revolution into tomorrow's norm.

Of course, there will be successes and failures in areas of hardware, software, networks, and societal acceptance along the way, but like all ecosystems, the best designs and approaches will thrive and eventually achieve equilibrium.

We expect IoT will grow in clusters, where various use cases and their related devices, applications, and connectivity shape their ecosystem. While these clusters begin to arise, there will be a natural tendency for them to try to link to other like clusters. As "clusters of clusters" start to crystallize, standards and regulations will emerge to enhance their ability to work together on a common platform.

1 INTRODUCTION

1.1 DEFINITIONS

Since there is not an “internet” exclusively dedicated to “things”, the expression “Internet of Things (IoT)” is best understood as a metaphor that encapsulates the immersion of almost anything and everything (previously “out of scope”) into the communications space thanks to the timely convergence of scientific, technological, and societal advances and trends.

The use of electronics, software, actuators, sensors and network connectivity allows “things” to collect and exchange data and, when programmed properly and designed in an accessible manner, allows citizens to make decisions on actions (automation) that can be enabled on/in a smart phone, vehicle, machine, home, community, city, etc.

In short, the "Internet of Things" (IoT) is about the interconnection of intelligent things. While interconnection (and its related and yet different concepts such as interoperability and interdependence) is axiomatic to IoT and a non-trivial building block, the intelligence of things (as a matter of course) is what makes the IoT paradigm “game-changing” [2,3]

As the European Research Cluster on the Internet of Things (IERC) puts it, IoT is:

> *“A dynamic global network infrastructure with self-configuring capabilities based on standards and interoperable communication protocols where physical and virtual things: have identities, physical attributes and virtual personalities; use intelligent interfaces; and are seamlessly integrated into the information network.”*[4]

[2] Center for the Development and Application of Internet of Things Technologies [CDAIT] Website (n.d.). *About - The Internet of Things.* Georgia Institute of Technology. Retrieved from https://cdait.gatech.edu/internet-things-infrastructure. A brief overview of IoT research and related perspectives at Georgia Tech can be found in Josh Brown, “Connected New World,” Georgia Tech Research Horizons, March 8, 2018 http://www.rh.gatech.edu/features/connected-new-world.

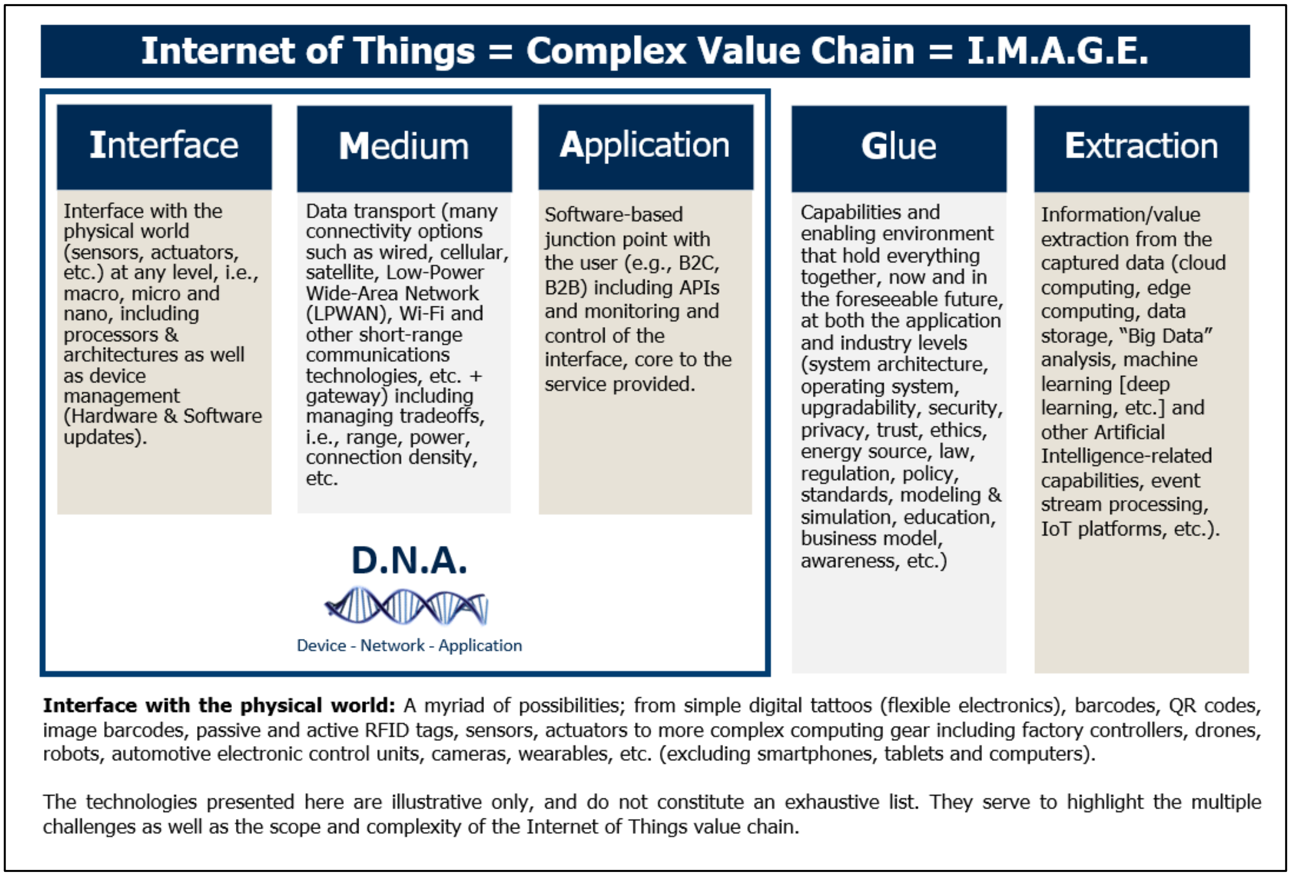
[3] A very insightful and useful collection of perspectives on the Internet of Things can be found in: Datta, S. (2017) *Haphazard Reality - IoT is a Metaphor: Principles and Practice of Connectivity and Convergence.* MIT Library https://dspace.mit.edu/handle/1721.1/111021

[4] European Research Cluster on the Internet of Things (IERC) website: http://www.internet-of-things-research.eu/about_iot.htm

This IoT network infrastructure is a complex, multilayered value chain composed of many moving parts as described in the IMAGE model below (Figure 1).

Looking at IMAGE, it is not difficult to see that IoT is bound to overhaul the way business was traditionally done (including possibly involving a new set of partners): IoT solutions require a kaleidoscope of new skills and expertise while at the same time causing the relationship with customers to profoundly change.[5]

[5] See Scott Ferguson, “Stanley Black & Decker CIO Drills Down Into Industrial IoT,” Light Reading, January 22, 2018 https://www.lightreading.com/enterprise-cloud/iot-and-edge/stanley-black-and-decker-cio-drills-down-into-industrial-iot/a/d-id/739658 and this comment from Stanley Black and Decker CIO Rhonda Gass:*"We're traditionally a mechanical/electrical engineering company, and we're now adding software skill-sets into our products," Gass said. "We're delivering IoT-enabled drills, or Bluetooth-enabled drills. What are the concerns around cybersecurity in that space that our traditional engineers are not used to thinking about? The IT group is assisting in helping put some of those policies and practices in place as well."*
See Mike Cushin, “Georgia-Pacific IoT Ecosystem Leader Breaks Down Intrapreneurship”, Enterprise Innovation website, n.d., http://www.enterpriseinnovation.com/articles/georgia-pacifics-iot-leader-breaks-down-intrapreneurship/ and this comment from Georgia Pacific IoT Ecosystem Leader, New Venture Development Mike Slawson*; “In the end, if we can lower our customers’ costs and help them use less of the products that we sell them, we become a more valuable supplier. This increases loyalty, reduces supplier churn, and helps us expand into more locations. We and our customers become more profitable. IoT is an important vehicle to accomplish this.”*
See Henk Volberda, Frans A.J. Van Den Bosch, and Kevin Heij, “Reinventing Business Models: How Firms Cope with Disruption,” (Oxford, UK,: Oxford University Press, 2017), p. 240: *“The leading tyre manufacturer Michelin, for instance, invested heavily in a new disruptive technology, namely the Internet of Things, and collaborated with completely new partners. With smart sensors and in-vehicle telematics, Michelin is no longer selling tyres, but also providing solutions for fleets of trucks, buses, and commercial vehicles in a wide range of areas: tyre management, vehicle productivity, and fuel efficiency.”*
See Paula Bernier, “New IoT Champion: Dell Commits to the Internet of Things,” IoT Evolution, February 2, 2018, http://www.iotevolutionworld.com/iot/articles/436793-new-iot-champion-dell-commits-the-internet-things.htm and this comment: Said [new IoT division leader Ray] O’Farrell. *“Our new IoT Division will leverage the strength across all of Dell Technologies’ family of businesses to ensure we deliver the right solution – in combination with our vast partner ecosystem – to meet customer needs and help them deploy integrated IoT systems with greater ease.”*
See IMAGE at work: an example of operational transformation as a result of IoT technologies can be found here: Jay Moye, “Connected Coolers: How the ‘Internet of Things’ is Powering Coke’s Fleet of Cold Drink Equipment,” Coca-Cola Journey website, March 20, 2018 https://www.coca-colacompany.com/stories/connected-coolers-how-the-internet-of-things-is-powering-coke-s-fleet-of-cold-drink-equipment
Industry collaboration brought about by the Internet of Things is highlighted in this 2016 Corning blog about the partnership between Corning and Samsung: “Jeff Evenson takes the stage at CES - Corning helps create a connected life in one of world’s most powerful trends,” Corning website https://www.corning.com/worldwide/en/innovation/the-glass-age/the-glass-age-today/ces-2016/jeff-evenson-takes-the-stage-at-ces.html - Note this statement from Dr. W.P. Hong, president of Samsung SDS, the company’s IT services subsidiary: *“Partnerships are the underpinning of IoT success”.*



Internet of Things = Complex Value Chain = I.M.A.G.E.

Interface

Interface with the physical world (sensors, actuators, etc.) at any level, i.e., macro, micro and nano, including processors & architectures as well as device management (Hardware & Software updates).

Medium

Data transport (many connectivity options such as wired, cellular, satellite, Low-Power Wide-Area Network (LPWAN), Wi-Fi and other short-range communications technologies, etc. + gateway) including managing tradeoffs, i.e., range, power, connection density, etc.

Application

Software-based junction point with the user (e.g., B2C, B2B) including APIs and monitoring and control of the interface, core to the service provided.

Glue

Capabilities and enabling environment that hold everything together, now and in the foreseeable future, at both the application and industry levels (system architecture, operating system, upgradability, security, privacy, trust, ethics, energy source, law, regulation, policy, standards, modeling & simulation, education, business model, awareness, etc.)

Extraction

Information/value extraction from the captured data (cloud computing, edge computing, data storage, "Big Data" analysis, machine learning [deep learning, etc.] and other Artificial Intelligence-related capabilities, event stream processing, IoT platforms, etc.).

D.N.A.

Device - Network - Application

Interface with the physical world: A myriad of possibilities; from simple digital tattoos (flexible electronics), barcodes, QR codes, image barcodes, passive and active RFID tags, sensors, actuators to more complex computing gear including factory controllers, drones, robots, automotive electronic control units, cameras, wearables, etc. (excluding smartphones, tablets and computers).

The technologies presented here are illustrative only, and do not constitute an exhaustive list. They serve to highlight the multiple challenges as well as the scope and complexity of the Internet of Things value chain.

Figure 1: IMAGE model of the IoT value chain[6]

Initially, IoT adoption will be implemented in small, independent installations. However, additional value is created when these individual applications can communicate with each other. By focusing on interoperability, IoT designers will be able to implement small clusters that can communicate with other clusters and further grow IoT toward the multi-trillion dollar global opportunity that is often mentioned.

However, the ability for these applications to share data is not necessarily straightforward. There are security and privacy issues, as well as governance and standards challenges, that stand in the way of seamless implementation.

Hence, this paper includes system considerations such as privacy, security, data ownership, technology integration, and universal (inclusive) design. IoT has the potential to go beyond just connecting individuals with their work, home, and other environments, but also supporting employment, community participation, and enhanced quality of life. A recent Tata Communications White Paper on the Internet of Things summarizes well this transformational paradigm:

> *"The Internet of Things presents an opportunity to transform society and establish a new ecosystem built to serve not merely humans, but humanity. In this new world, people will receive uniquely personalised services on demand, while societies will*

[6] Source: Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT)

> *benefit from optimised resource use and minimised negative environmental impact. The Organisation for Economic Co-operation and Development (OECD) compares IoT's significance and potential ubiquity to the advent of household electricity and sees it extending beyond technology and commerce to redefine our social, cultural and professional relationships."*[7]

Inclusive IoT seeks to create a more connected society by integrating *Design Thinking* (see Section 5.5 below) and policy development approaches to better match technological applications to citizen needs and determining how best to design solutions that bridge technological and societal gaps. While municipalities can harness the wide range of IoT technologies to enable employees to be more efficient and effective (boosting productivity), an equally interesting goal is to use these technologies to enhance the citizen experience. This is one of the most innovative approaches to ensuring the effective and efficient uptake of IoT – devising novel ways to provide meaningful and rewarding citizen engagement.[8]

It is becoming increasingly clear that traditional business models are dislocated by the arrival of the Internet of Things. For instance, thanks to IoT technologies, capital expenditures are now becoming operational expenses through "as-a-service"-based purchase options. In addition, a typical IoT solution requires expertise in many domains and forces companies to collaborate and share revenue.[9]

Ultimately, IoT will be a boon for cities as they partner with the technology community to support their growing populations and developing domestic and global economies. In the process, cities will transform into "Smart Cities" (see section 2.1 below for definition).

As leaders in Smart Cities establish the digital infrastructure needed to enable municipal and service provider innovations, they must also consider how to reduce the risk of data leakage and function creep.[10]

Municipalities should incorporate risk management procedures into their Smart City procurement process to ensure that adequate security measures are in place for the lifecycle of the technology and look to address privacy and security concerns by embedding design practices throughout the public service delivery process. Municipalities won't be alone in

[7] Tata Communications, "India IoT Report – Emergence of a New Civic OS [Operating System]", February 2018, p.5, https://www.tatacommunications.com/wp-content/uploads/2018/02/IoT-Report.pdf - Note: the OECD source is: Organisation for Economic Co-operation and Development (OECD), "The Internet of Things: Seizing the benefits and addressing the challenges", May 2016, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP%282015%293/FINAL&docLanguage=En..

[8] See research done on "Smart Cities and Inclusive Innovation" at Georgia Tech.

[9] The almost 2300 IoT meetup groups around the world and their approximately 1.3 million members (as of June 2018) - see https://www.meetup.com/topics/internet-of-things/ are perhaps altogether another concrete indication of the IoT interdependence and the need for "interdisciplinary" and "intermarket" perspectives. As an example, see GAIT - Greater Atlanta Internet of Things Meetup for people interested in the Internet of Things who want "to collaborate on new ideas and lessons learned to raise up the entire community," which keeps exploring a broad variety of technologies and domains in IoT https://www.meetup.com/Greater-Atlanta-Internet-of-Things/

[10] See Bruce Schneier, "Security and Function Creep", IEEE Security and Privacy, January/February 2010, https://www.schneier.com/essays/archives/2010/01/security_and_functio.html

this. The opportunity to participate in the financial benefits associated with Smart Cities will drive technology companies to seek solutions and remedies to current challenges. In the process, substantial transformative changes will upset the status-quo:

> *"It's hard to imagine the future of IoT, but it's clear that it will create entirely new markets and bring massive disruption to existing markets. When the physical world and online world come together, every business venture becomes, to some degree, a software and data company."*[11]

1.2 IoT Dimensions

There is a plethora of IoT projections constantly renewed and adjusted, but all are pointing to an "undeniable trend", i.e., a fast expanding and huge market[12,13]. The technological, economic, and socioeconomic potentials of IoT affords various industries the opportunity to solve numerous problems and are therefore key to IoT's value proposition.

IoT has received increased attention in the last few years as a result of timely converging trends, such as market and technology obsolescence (e.g., legacy voice and data service revenue decline)[14]; cost-effective and efficient miniaturization of sensors, actuators, radio modules, and other interfaces with the physical world[15]; a dramatic jump in the number of

[11] Blake Patton, Tech Square Ventures and Chair of the CDAIT Working Group on the IoT Startup Ecosystem. Source: Interview for Venture Atlanta, February 2015, https://techsquareventures.com/blake-patton-security-disruption-internet-things-venture-atlanta/

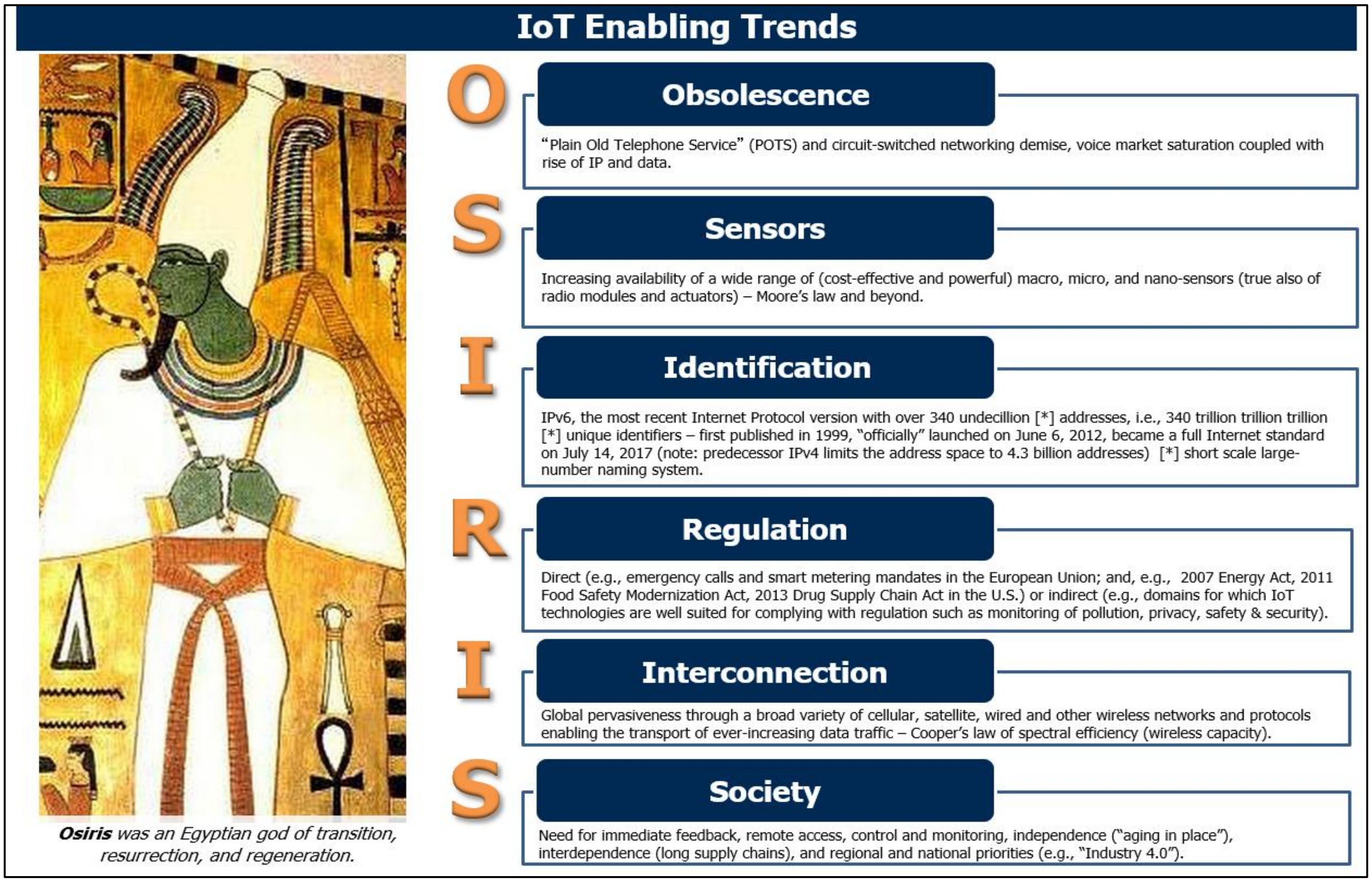
[12] Unlocking the potential of the Internet of Things, *McKinsey and Company,* June 2015, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[13] Amy Nordrum, IEEE Spectrum, 18 August 2016, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated". Let's note as Amy Nordrum points out that "one of the puzzling things about IoT estimates is that they attempt to anticipate demand for devices that have largely not yet been invented or commercialized."

[14] See Tina Gurnaney, "IoT may rescue telcos when revenues from voice and data services decline: Analysts," India Times, August 30, 2017 https://telecom.economictimes.indiatimes.com/news/iot-may-rescue-telcos-when-revenues-from-voice-and-data-services-decline-analysts/60227229; Martin Creaner's Interview at Mack Institute News, Wharton, University of Pennsylvania, "The Future of Telecoms in the IoT Era," February 19, 2016 https://mackinstitute.wharton.upenn.edu/2016/the-future-of-telecom-in-the-iot-era/ ; and Astrid Rauchfuss et al."To Fuel Growth, Telcos Need a Digital Makeover," BCG, April 12, 2018 https://www.bcg.com/publications/2018/to-fuel-growth-telcos-need-digital-makeover.aspx. On June 5, 2018, Juniper Research issued a press release that highlighted that "annual global operator-billed revenues from voice and data services are expected to fall by over $50 billion over the next 5 years from $836 billion last year [2017] to $785 billion by 2022" and "that the opportunities afforded by the IoT (Internet of Things) should enable operators to increase revenues from that sector by over $8 billion by 2022." https://www.businesswire.com/news/home/20180605005133/en/Juniper-Research-Mobile-Operator-Core-Revenues-Fall

[15] Note that cost-effective miniaturization, i.e., a critical catalyst of the IoT expansion, includes a vast number of technologies that have progressed by leaps and bounds in the last decade; a handful of examples: flexible electronics, Shoubhik Gupta et al. "Ultra-thin chips for high-performance flexible electronics," Nature, March 2018, https://www.nature.com/articles/s41528-018-0021-5; High Density Interconnect (HDI) Printed Circuit Board (PCB), iFastPCBBlog,"The Quiet Mainstreaming of HDI PCB Manufacturing," August 2, 2016 http://www.ifastpcb.com/blog/the-quiet-mainstreaming-of-hdi-pcb-manufacturing/ ; and efficient energy source, Yunlong Zi and Zhong Lin Wang, "Nanogenerators: An emerging technology towards nanoenergy," APL Materials, March 2017 https://aip.scitation.org/doi/full/10.1063/1.4977208 and Anne Trafton, "Wireless

available internet addresses (IPv6 vs. IPv4[16]); regulations around the world conducive to the use of IoT technologies[17]; growing pervasive interconnection capabilities[18]; and favorable societal needs and requirements[19], as described in the high-level OSIRIS representation below (Figure 2). The accompanying Figure 3 provides historical context to IoT.



IoT Enabling Trends

O — Obsolescence

"Plain Old Telephone Service" (POTS) and circuit-switched networking demise, voice market saturation coupled with rise of IP and data.

S — Sensors

Increasing availability of a wide range of (cost-effective and powerful) macro, micro, and nano-sensors (true also of radio modules and actuators) – Moore's law and beyond.

I — Identification

IPv6, the most recent Internet Protocol version with over 340 undecillion [*] addresses, i.e., 340 trillion trillion trillion [*] unique identifiers – first published in 1999, "officially" launched on June 6, 2012, became a full Internet standard on July 14, 2017 (note: predecessor IPv4 limits the address space to 4.3 billion addresses) [*] short scale large-number naming system.

R — Regulation

Direct (e.g., emergency calls and smart metering mandates in the European Union; and, e.g., 2007 Energy Act, 2011 Food Safety Modernization Act, 2013 Drug Supply Chain Act in the U.S.) or indirect (e.g., domains for which IoT technologies are well suited for complying with regulation such as monitoring of pollution, privacy, safety & security).

I — Interconnection

Global pervasiveness through a broad variety of cellular, satellite, wired and other wireless networks and protocols enabling the transport of ever-increasing data traffic – Cooper's law of spectral efficiency (wireless capacity).

S — Society

Need for immediate feedback, remote access, control and monitoring, independence ("aging in place"), interdependence (long supply chains), and regional and national priorities (e.g., "Industry 4.0").

***Osiris** was an Egyptian god of transition, resurrection, and regeneration.*

Figure 2: OSIRIS representation of enabling trends that have driven IoT adoption [20]

system can power devices inside the body," MIT News, June 4, 2018, https://news.mit.edu/2018/wireless-system-power-devices-inside-body-0604

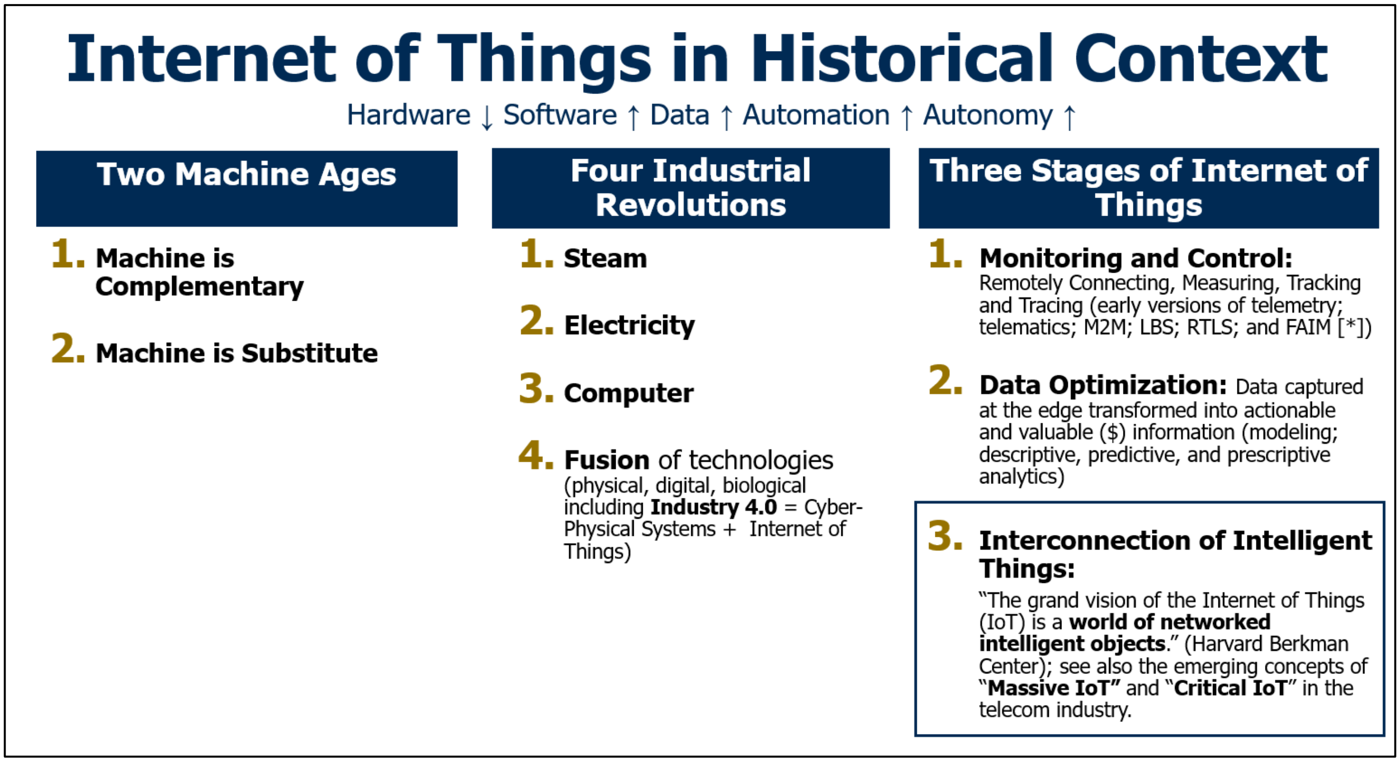
[16] Sébastien Ziegler et al. "The Case for IPv6 as an Enabler of the Internet of Things," IEEE Newsletter, July 14, 2015 https://iot.ieee.org/newsletter/july-2015/the-case-for-ipv6-as-an-enabler-of-the-internet-of-things.html

[17] See how IoT technologies can help with air quality monitoring as "many countries across Europe including the UK, Germany, France, Italy and Spain face the prospect of huge fines arising from persistent failures to comply with European air pollution laws," in GSMA, "Air Quality Monitoring Using IoT and Big Data - A Value Generation Guide for Mobile Operators, " February 2018 https://www.gsma.com/iot/wp-content/uploads/2018/02/iot_clean_air_02_18.pdf

[18] For a recent overview of IoT interconnection challenges and drivers see Prof. Mustapha Benjillali's presentation on "Interoperability, Integration, and Interconnection of Internet of Things Systems," at the ITU-SUDACAD Regional Forum - IoT for Development of Smart Sustainable Cities, Khartoum, Sudan, December 13-14, 2017 https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/IoTSMW/Presentations-IoT/Session6/IoT4SSC_Session_6_Benjillali.pdf

[19] See for example Sheik Mohammad Mostakim Fattah et al., "Building IoT Services for Aging in Place Using Standard-Based IoT Platforms and Heterogeneous IoT Products," Sensors 2017, 17(10), 2311; https://doi.org/10.3390/s17102311

[20] Source: Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT)



Internet of Things in Historical Context

Hardware ↓ Software ↑ Data ↑ Automation ↑ Autonomy ↑

Two Machine Ages

1. **Machine is Complementary**
2. **Machine is Substitute**

Four Industrial Revolutions

1. **Steam**
2. **Electricity**
3. **Computer**
4. **Fusion** of technologies (physical, digital, biological including **Industry 4.0** = Cyber-Physical Systems + Internet of Things)

Three Stages of Internet of Things

1. **Monitoring and Control:** Remotely Connecting, Measuring, Tracking and Tracing (early versions of telemetry; telematics; M2M; LBS; RTLS; and FAIM [*])
2. **Data Optimization:** Data captured at the edge transformed into actionable and valuable ($) information (modeling; descriptive, predictive, and prescriptive analytics)
3. **Interconnection of Intelligent Things:** "The grand vision of the Internet of Things (IoT) is a **world of networked intelligent objects**." (Harvard Berkman Center); see also the emerging concepts of "**Massive IoT"** and "**Critical IoT**" in the telecom industry.

Figure 3: IoT in Historical Context[21]

*[*] **Telemetry** is the automatic measurement and wireless transmission of data from remote sources; [Vehicle] **telematics** refers to the gathering, storing, and transmitting of data about a vehicle(s) for monitoring purposes; **M2M**= Machine-to-Machine communications; **LBS** = Location-Based Service; **RTLS** = Real-time Locating System; **FAIM** = Flexible Automation and Intelligent Manufacturing (note: the annual FAIM conference was first hosted in 1991 by the University of Limerick, Ireland and has been held uninterruptedly around the world since then.)*

IoT technologies have the potential to solve a number of problems for consumers, businesses, government entities and academic units, at a reasonable cost. Ultimately, the technologies must have enough "pull" from society, the end users/consumers, and government so that they are adopted and, in the process, foster citizen engagement.

[21] Source: Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT) - based on and adapted from various sources including Paul Kominers (April 1, 2012), "Interoperability Case Study: Internet of Things (IoT)," Berkman Center for Internet and Society, Harvard University; Brynjolfsson, E., and McAfee, A. (2014), "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies," New York, NY: WW Norton & Company; Centre for Strategy and Evaluation Services LLP (CSES) (2016), "Study on Industry 4.0," prepared for the European Parliament's Committee on Industry, Research and Energy (ITRE); Yuval Noah Harari (2016), "Homo Deus: A Brief History of Tomorrow," London, U.K.: Harvill Secker; Shwab, K. (2017), "The Fourth Industrial Revolution," New York, NY: Crown Business; Husain, A. (2017), "The Sentient Machine: The Coming Age of Artificial Intelligence," New York, N.Y.: Scribner; 5G Americas (December 2017), "LTE Progress Leading to the 5G Massive Internet of Things"; Akpakwua, G. A. et al. (February 2018) "Survey on 5G networks for the internet of things: communication technologies and challenges," IEEE Access, Volume 6, 2018; and Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT) Website (n.d.). About - The Internet of Things, Georgia Institute of Technology.

As recently argued by international research firm Gartner, "citizen engagement and the enhancement of services and experience will be critical to the success of smart cities."[22]

Prior to gaining customer "buy in", there are additional requirements for market entry that IoT must address, including:

1. Governance/standards on privacy and security
2. Solutions to questions on the impact of adoption and data ownership on citizens
3. Governance to ensure ALL people are able to actively and consciously participate
4. Commercial implementation readiness of technologies
5. Universal /interoperable platforms/ systems
6. Cost-effective solutions
7. Other standards (e.g. networking, data exchange, etc.)

As an example, the recent data breaches at Yahoo (500 million accounts stolen; 3 months later, 1 billion accounts affected), Equifax (143 million Americans compromised) and Target (40 million shoppers affected), demonstrate how consumers can be immediately impacted by hacking. Without the proper standards and system governance in place, it is difficult to minimize the risk to families and communities from this type of criminal activity.[23] These types of breaches can also have immediate consequences due to both the negative impact on citizens as well as the impact on corporate valuations. Due to the security breach, Yahoo

[22] See SmartCitiesWorld, "Citizen engagement is key to Smart City success," March 8, 2018, https://smartcitiesworld.net/news/citizen-engagement-is-key-to-smart-city-success-2685

[23] "The Biggest Data Breaches Ever," Seth Fiegerman, @SFiegerman, September 7, 2017, http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html. See also Dennis Green, "If you shopped at these 14 stores in the last year, your data might have been stolen", April 6, 2018, http://www.businessinsider.com/data-breaches-2018-4. Although technically not a hack, Cambridge Analytica's harvest between 2013 and 2015 of profile data from millions of Facebook users, without those users' permission, is also a vivid example of privacy invasion risk. See Aja Romano, "The Facebook data breach wasn't a hack. It was a wake-up call.", March 10, 2018, https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained.
Note: Regarding recent data breaches and perspectives on cybersecurity risks, the Verizon 2018 Data Breach Investigations Report (11th edition) is available here: https://www.verizonenterprise.com/verizon-insights-lab/dbir/; the AT&T 2018 Cybersecurity Insights Report (Vol. 7) is available here: https://www.business.att.com/content/whitepaper/cybersecurity-report/v7/index.html ; the Cisco 2018 Annual Cybersecurity Report is available here: https://www.cisco.com/c/en/us/products/security/security-reports.html; the 2018 IBM X-Force Threat Intelligence Index is available here: https://www.securitymagazine.com/articles/88893-ibm-x-force-report-fewer-records-breached-in-2017, the report "Putting Industrial Cyber Security at the Top of the CEO Agenda' released by Honeywell in December 2017 is available here: https://www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-of-industrial-cyber-security-measures.aspx; and the Georgia Tech Emerging Cyber Threats, Trends and Technologies 2017-18 report is available here: https://cyber.gatech.edu/threats-reports

took a direct hit on company value when Verizon reduced the price of its deal to buy Yahoo by $350 million. [24]

U.S. House of Representatives Resolution 847

"Expressing the sense of the House of Representatives about a national strategy for the Internet of Things to promote economic growth and consumer empowerment."

September 12, 2016

"…[I]t is the sense of the House of Representatives that the United States should develop a national strategy to encourage the development of the Internet of Things in a way that maximizes the promise connected technologies hold to empower consumers, foster future economic growth, and improve the Nation's collective social well-being."

We must also be cognizant of possible increases in societal inequalities, deepening the so-called *Digital Divide*. For example, there is a risk of taking advantage of ill/under-informed members of society. This could be for a variety of reasons: misunderstanding of the technology and/or data/information sharing, or even an inability to utilize the technology. Governments and industry must work together to create an environment where technological innovation can occur while the citizens are protected through regulation and education (including implementers' training).

In addition to governance standards, technological standards need to be created and adopted. Several organizations around the world (some may have various committees, subcommittees and working groups associated directly or indirectly to IoT) are developing IoT-related standards, specifications and test mechanisms such as, but not limited to 3GPP, Alliance for Telecommunications Industry Solutions [ATIS], American National Standards Institute [ANSI], Association of Radio Industries and Businesses [ARIB], Bluetooth Special Interest Group ("SIG"), CableLabs, China Communications Standards Association [CCSA], Dash 7 Alliance, Eclipse IoT (open source), EPC Global, FieldComm Group, European Telecommunications Standards Institute [ETSI], GSMA, Hypercat Alliance, Institute of Electrical and Electronics Engineers [IEEE], International Electrotechnical Commission [IEC], International Organization for Standardization [ISO], International Society of Automation [ISA], International Telecommunication Union [ITU], Internet Engineering Task Force [IETF], LoRA Alliance, National Institute of Standards and Technology [NIST], NFC Forum, oneM2M, OASIS, Open Connectivity Foundation [OCF], Open Geospatial Consortium [OGC], OMA SpecWorks, Object Management Group [OMG] [including the Industrial Internet Consortium

[24] https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/

[IIC], a non-standards forming program of OMG] , Open Alliance for IoT Standard [OCEAN], Open Connectivity Foundation [OCF], OPC Foundation, Open Group IoT Working Group, RFID Consortium, Standards Council of Canada (SCC), Telecommunications Industry Association [TIA], Telecommunications Technology Association [TTA], Telecommunications Technology Committee [TTC], Thread Group, TMForum, World Wide Web Consortium [W3C], Weightless SIG, Wi-SUN Alliance, Zigbee Alliance, and Z-Wave Alliance, Note that open source is rapidly establishing a wide footprint in IoT.[25].

Other alliances, associations, fora and similar groups are working on best practices, protocols and standards on elements of the IoT value chain (see Figure 1 IMAGE above), e.g., computing, data capture, privacy, security, etc.; or a specific industry (vertical market), e.g., agriculture, construction (including homes and commercial buildings), education, energy (including smart grid), environment, finance (including banking and insurance), lighting, manufacturing, smart cities, transportation, etc.

In parallel, substantial work is underway to identify existing IoT standards and their associated gaps in order to apprehend more accurately the present IoT standards landscape and build an overarching IoT framework.

Some examples of these efforts are:

- The IEEE P2413™ Draft IEEE Standard for an Architectural Framework for the Internet of Things (IoT), initiated by IEEE in 2014, which is designed to propose an architectural framework supporting cross-domain interaction, system interoperability and functional compatibility.[26]

- ISO/IEC Joint technical committee (JTC) 1/subcommittee (SC 41), which was created in 2017, focuses on the Internet of Things and related technologies, including sensor networks and wearables technologies. ISO/IEC JTC 1 (created in 1987) is a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) whose objective is to develop worldwide Information and Communication Technology (ICT) standards for business and consumer applications. The Secretariat for ISO/IEC JTC 1/SC 41 is the Korean Agency for Technology and Standards (KATS).[27]

- The U.S.-based InterNational Committee for Information Technology Standards through its Internet of Things committee (INCITS/IoT) endeavors among other objectives to monitor the ongoing IoT regulatory, market, business and technology

[25] Brian Buntz, “Open Source IoT Is Growing in Importance,” Internet of Things Institute, May 24, 2018 https://www.ioti.com/strategy/open-source-iot-growing-importance - See also Stephen Hendrick, “ The Impact of Open Source Software on Developing IoT Solutions ,” RT Insights, March 2, 2018 https://www.rtinsights.com/the-impact-of-open-source-software-on-developing-iot-solutions/ and Jeff Evans and Alain Louchez, “Could Open Source Be An Engine For The Internet Of Things?” MNET, March 4, 2014 https://www.manufacturing.net/article/2014/03/could-open-source-be-engine-internet-things

[26] See: https://standards.ieee.org/develop/wg/IoT_Architecture.html and Beyond Standards, IEEE, “What Is Open Source, and Why Is IEEE Involved?” May 2, 2017 https://beyondstandards.ieee.org/general-news/open-source-ieee-involved/

[27] See https://www.iso.org/committee/6483279.html

requirements. INCITS/IoT addresses standardization in the areas assigned to ISO/IEC JTC 1 SC 41. INCITS / SG-IoT's first organizational meeting was held on February 27, 2013.[28]

- The International Telecommunication Union (ITU) Study Group (SG) 20[29] Internet of Things (IoT) and smart cities and communities (SC&C)'s work on IoT and SC&C roadmap. ITU SG 20 was created by the Telecommunication Standardization Advisory Group (TSAG) at its meeting at ITU Headquarters in Geneva, June 2-5, 2015.

- In May 2016, the U.S. National Institute of Standards and Technology (NIST) published its "Framework for Cyber-Physical Systems – Release 1.0", following the publication in February 2016 of the "Current Standards Landscape for Smart Manufacturing Systems". NIST views Cyber-physical systems (CPS) as smart systems that include engineered interacting networks of physical and computational components and points out that in addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) that describe similar or related systems and concepts.[30]

- In June 2017, the IoT European Research Cluster (IERC) published the eighth edition of the Cluster book "Cognitive Hyperconnected Digital Transformation - Internet of Things Intelligence Evolution". Chapter 6 is entirely focused on "IoT Standards Landscape – State of the Art - Analysis and Evolution" and includes a section on gaps in IoT standardization.[31]

- The European Union's Alliance for Internet of Things Innovation (AIOTI) Working Group 3 – See one of their most recent publications as of this writing related to IoT standards gaps: "High Priority IoT Standardization Gaps and Relevant SDOs [Standards Developing Organizations]," Version 1.0, May 2018[32] and the very-well documented "IoT LSP [Large Scale Pilot] Standard Framework Concepts Release 2.8", February 8, 2017.[33]

[28] See http://www.incits.org/committees/internet-of-things and Chuck Adams, Convenor, "INCITS Study Group Internet of Things," INCITS Plenary Report, April 18, 2013 Note that the International Committee for Information Technology Standards (INCITS) is an ANSI-accredited standards developing organization and the U.S. Technical Advisory Group (TAG) Administrator of ISO/IEC JTC 1.

[29] See website here: https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

[30] The CPS framework is available here https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf
The smart manufacturing systems landscape is available here: Y. Lu, K. Morris, and S. Frechette, "Current standards landscape for smart manufacturing systems," National Institute of Standards and Technology, NISTIR vol. 8107, February 2016, available at https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf

[31] The IERC - IoT European Research Cluster - European Research Cluster on the Internet of Things is bringing together EU-funded projects with the aim of defining a common vision and the IoT technology and development research challenges at the European level in the view of global development. The book is available at http://www.internet-of-things-research.eu/pdf/Cognitive_Hyperconnected_Digital_Transformation_IERC_2017_Cluster_eBook_978-87-93609-10-5_P_Web.pdf

[32] Available at https://aioti.eu/wp-content/uploads/2018/05/AIOTI-WG3_High_Priority_Gaps_v1.0_final.pdf

[33] Available at https://aioti.eu/wp-content/uploads/2017/06/AIOTI-WG3_sdos_alliances_landscape_-_iot_lsp_standard_framework_concepts_-_release_2_v8.pdf

- In March 2018, the German Standardization Council Industrie 4.0 (SCI 4.0) published a report on the German Standardization Roadmap, Industry 4.0, Version 3, which provides an insightful picture on various international standardization efforts related to what is known as the "Industrial Internet of Things".[34]
- The European Union's H2020-UNIFY-IoT Project[35] is the "working partner" of the Alliance for Internet of Things Innovation (AIOTI) and the Internet of Things European Research Cluster (IERC) by coordinating and supporting the activities on innovation ecosystems, IoT standardization, Policy Issues, Research and Innovation.

Incidentally, the Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT) has a Standards and Management Working Group dedicated to analyzing key IoT-related standards efforts in relation to how they will interact with each other; affect the implementation of IoT solutions; and, eventually, impact business performance.[36]

1.3 Paper Objectives

In order to address IoT and its rapidly growing set of innovations, this paper applies four critical questions to four use cases with Smart Cities as a representative IoT vertical market ("the case in point").

The questions are:

1. What are the opportunities for, and limits of, Smart Cities and connected users/communities?
2. What are the data ownership and security issues, and how will they be addressed?
3. What will IoT business models look like and what would constitute "success"?
4. What possible roadmaps can lead to the IoT revolution becoming the IoT of the future?

The five key use cases are:

1. Municipal Services Management: Effective interaction with the citizens
2. Utilities: Water, waste, smart electric grid.
3. Public Safety: Public care, safe city, amenity services (fire, police)
4. Transportation: Traffic, lighting, parking, safety.
5. Healthcare: Hospitals, home care, emergency services

[34] In April 2016, the "Standardization Council Industrie 4.0" (SCI 4.0) was co-founded by the German Association for Information Technology, Telecommunications and New Media (Bitkom), German Institute for Standardization (DIN), German Commission for Electrical, Electronic & Information Technologies (DKE), German Engineering Federation (VDMA) and Central Association of the Electrical Engineering and Electronics Industry (ZVEI). The report is available at https://www.din.de/blob/65354/57218767bd6da1927b181b9f2a0d5b39/roadmap-i4-0-e-data.pdf

[35] See March 23, 2018 report on "Interoperable IoT Platforms – Standards Framework": http://www.unify-iot.eu/wp-content/uploads/2018/04/D05_02_WP05_H2020_UNIFY-IoT_Final.pdf

[36] At the time of this writing: Robert Kamp (Intel) – chair, Daniel Walton (Cisco) – vice chair, and Bill Eason (Georgia Tech).

2 Question 1: Smart Cities Opportunities and Limits

WHAT ARE THE OPPORTUNITIES FOR, AND LIMITS OF, SMART CITIES AND CONNECTED USERS/COMMUNITIES?

2.1 Introduction

The rapidly accelerating degree of access to information and services made possible by digital technology and Internet of Things (IoT) connectivity has promising potential for generating economic and social benefits, but it also raises some significant issues that need to be resolved as IoT systems are designed and deployed.

This includes addressable issues that are relatively straightforward (regulatory requirements, adoption-related issues, etc.) as well as "big picture" and future-use scenarios that can drive development and implementation approaches. Much of the initial focus has been on the supply side – the technology involved in the implementation – and less on the needs and concerns of the ultimate beneficiaries of adoption – the human end users, citizens of the city. This is one of the key areas that is most in need of innovative non-linear thinking.

IoT has been referred to variously as a **platform** (in terms of software that bridges devices, sensors and data networks, e.g. platform as a service), **infrastructure** (the hardware, routers, fiber and internet protocols that provide the substrate that IoT rests on), **ecosystem** (broadly speaking, the objects and devices that allow users to connect to and use IoT, including applications, dashboards, analytics, networks, and industries that participate in the development and support of IoT), or **framework** (typically in reference to the policy and regulatory structures that impact IoT).[37] Given the preceding, a more nuanced approach to IoT design and deployment is called for – a design and implementation strategy that includes system considerations such as privacy, security, data ownership, technology integration, and universal (inclusive) design.

IoT has the potential to go beyond connecting individuals with their work, home, and other environments and, as cities morph into "Smart Cities", can support employment, community participation, and enhanced quality of life.

"Smart City" definitions vary widely. The following observations from the February 2018 draft from the National Institute of Standards and Technology (NIST) (at the U.S. Department of Commerce) and its partners in "A Consensus Framework for Smart City Architectures" offer a sound starting point:

> *"The Smart City can be defined as the integration of data and digital technologies into a strategic approach to sustainability, citizen well-being and economic development [Source: Urban Tide and Scottish Government, 2014]. A Smart City inspires the vision*

[37] Consumer Technology Association (CTA). (2016). *INTERNET OF THINGS: A Framework for the Next Administration*. November 2016. Washington D.C.: Consumer Technology Association https://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf

> *of a space where key components of infrastructure and services environmental, emergency response, traffic and energy management to name a few are integrated in such a way that features and applications can easily be combined with whatever capability existed before [Source: Taewoo Nam and Theresa A. Pardo, 2011]. Achieving that vision requires moving beyond many current implementations in which the degree of integration of core subsystems within Smart Cities is often limited by patchworks of legacy and fixed solutions connected by custom integrations."*[38]

2.2 IoT Stakeholders

IoT implementation in Smart Cities benefits different stakeholders in different ways – a wide range of end users encompassing citizens, visitors, and those merely passing through the physical envelope of the city.

Ultimately, IoT-facilitated benefits must be perceived to be of value to the end-user stakeholder, but a second key stakeholder is the institutional adopter– the municipality, governmental and organizational decision maker. These decision makers are tasked with articulating and implementing an IoT strategy based on the needs of the citizens, an understanding of parameters of city operations, and the allocation of public funds to pay for IoT deployment. A third major stakeholder group encompasses private and industry interests – these range from businesses operating within the city, to technology and system vendors (for IoT), to the information carriers (the wireless and technological providers that make IoT operational). Regardless of the specifics of an IoT infrastructure, system design needs to address the key objectives of enhanced living experience and time savings, reduced demand on transportation infrastructure, a more-informed citizenry, and, with the enhanced information made possible by IoT, better decision making by governments.

With an eye toward increasing the utility of IoT for end users, other aspects that need to be considered are the accessibility and usability of these technologies, which can increase participation for a great number of users. This is a typically overlooked design component and one that designers and developers of Smart City-connected applications, devices, and technologies could facilitate by obtaining input from a wide range of users, especially those who could potentially benefit the most from IoT technologies: people with disabilities, the aging, minorities/underrepresented groups, and other underserved populations. To date, there has been much research seeking to understand the relationship between disability status and information and communication technologies (ICT), while exploring policies that may help bridge the digital gap between people with disabilities and the rest of the

[38] See Internet-of-Things Enabled Smart City Framework (a.k.a. IES-City Framework), released by the National Institute of Standards and Technology (NIST) on February 8, 2018, p. 1 https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFrameworkdraft_20180207.pdf - The written statement of Dr. Jennifer Clark, Director of the Georgia Tech Center for Urban Innovation (https://urbaninnovation.gatech.edu/), which accompanied her testimony before the U.S. Congress on March 16, 2017, provides useful perspectives on the Smart City concept – see http://docs.house.gov/meetings/IF/IF17/20170316/105710/HHRG-115-IF17-Wstate-ClarkJ-20170316.pdf

population[39,40]. The insights generated from IoT data streams could profoundly enhance the advancement of that knowledge.

In the rush to build the "Brave New Connected World", the technology must be flexible enough to serve the needs of various users or run the risk of leaving behind some of the most vulnerable members of society. *Inclusive IoT* bridges the many aspects of a connected society by integrating design thinking and policy development approaches to better match technology to citizen needs and determine how best to design appropriate measures to bridge technological gaps.

Toronto's Chief Digital Transformation Officer Michael Kolm sums up the current Smart City challenges this way:

> *"If Smart City 1.0 was about the technology, Smart City 2.0 is about the social and economic perspectives."*[41]

2.3 DEPLOYMENT CONSIDERATIONS, OPPORTUNITIES, AND LIMITS

The opportunities and benefits of IoT detailed above (and relatively well discussed in the academic and trade literature) include issues of accessibility, usability, total cost of ownership (including cost of implementation as well as cost of operation and maintenance), data collection and processing, sustainability, and training for users. From a design standpoint, possible barriers to adoption such as security and privacy, regulatory constraints, and user friendliness, among others must be taken into account. They can have significant impact on the value proposition that municipalities review.

Not surprisingly, an examination of IoT deployments in US cities does not really result in a set of overall "best cities", but rather novel and effective applications of IoT within specific use cases. A significant problem, though also an opportunity for innovative design, is that many of the U.S. cases are pilot projects, specialized uses or based on the specifics of a vendor-centric IoT platform and technologies.

Fortunately, there is a wide swath of organizations and initiatives around the world that shape best practices and standards, and identify lessons learned for the benefit of Smart City stakeholders. A few examples are given here without any order of priority: Alliance for Telecommunications Industry Solutions (ATIS) [Smart Cities Technology Roadmap], Smart Cities Council, AIOTI Working Group 08 on Smart Cities, IEEE Smart Cities, IEEE 2413.1-

[39] Goggin, G., & Newell, C. (2003). *Digital disability: The social construction of disability in new media*: Rowman & Littlefield.

[40] Gunn, A., & Mintrom, M. (2016). Higher Education Policy Change in Europe: Academic Research Funding and the Impact Agenda. *European Education*, 48(4), 241-257.

[41] In Andy Caham, "Smart Cities Are About Helping People, Civic Leaders Agree", Digitalist Magazine, May 9, 2018, http://www.digitalistmag.com/improving-lives/2018/05/09/smart-cities-are-about-helping-people-civic-leaders-agree-06164054. In the same article, Caham concludes *"While smart cities might have once been about simply making things more efficient or introducing cool gadgets, there's now a new purpose: Using technology to tackle the biggest social and economic challenges faced by cities around the world. To echo the sentiment at the Smart Cities Forum, a city is nothing without its people, and it's nothing if it's not giving them all opportunities to succeed in the digital economy."*

Standard for a Reference Architecture for Smart City (RASC), the International Secure Smart and Resilient Cities Initiative (SSCI), International Telecommunication Union (ITU) SG 20, the World's Smart Cities Organizations (WSCO), World Smart City [ISO, IEC, ITU], U.S. National Institute of Standards and Technology (NIST) Smart Cities Framework, U.S. Department of Transportation Smart City Challenge, 100 Resilient Cities, Future Cities Catapult (UK), ANSI Network on Smart and Sustainable Cities (ANSSC), Cities Alliance, Global Future City Alliance (GFCA), Open & Agile Smart Cities (OASC), Georgia Smart Communities Challenge, etc.

It is noteworthy that under the State of Modern Application, Research, and Trends of IoT Act ("SMART IoT Act") [H.R.6032] currently under consideration in the U.S. Congress [see section 5.2 below] the Secretary of Commerce would develop and conduct a study containing "a description of the ways entities or industry sectors develop, use, or promote the use of internet-connected devices."

2.4 USE CASES

2.4.1 Municipal Services Management

Effective Interaction with the Citizens

The U.S. Code of Federal Regulations defines municipal services as follows (in a specific context, i.e., payments for municipal services in atomic energy communities):

> *"The term "municipal-type services" includes services usually rendered by a municipality and usually paid for by taxes. Examples of municipal-type services are police protection, fire protection, public recreational facilities, public libraries, public schools, public health, public welfare, and the maintenance of roads and streets. The term shall include sewage and refuse disposal which are maintained out of revenues derived from a general charge for municipal-type services; however, the term shall not include sewage and refuse disposal if a separate charge for such services is made."*[42]

However, there is no consensus on what municipal services are (or should be):

> *"Local authorities differ between countries in terms of their size, functions, degree of autonomy and objective."*[43]

While we look at specific "municipal-type services" in detail in the following sections, we examine here the side of the local administration that relates to its overarching catalytic role in promoting economic and social growth via efficient service delivery and effective citizen interaction in partnerships with the private sector and other alliances. Through this role, the

[42] 26 CFR 1.164-8 - Payments for municipal services in atomic energy communities https://www.gpo.gov/fdsys/pkg/CFR-1998-title26-vol2/xml/CFR-1998-title26-vol2-sec1-164-8.xml

[43] International Labour Organization (ILO), "The Impact of Decentralization and Privatization on Municipal Services," October 15-19, 2001, http://www.ilo.org/public/english/standards/relm/gb/docs/gb283/pdf/jmmsr.pdf

city is an enabler, i.e., a crucible for business and technological innovation at the service of its citizens.

A number of analysts foresee a growing population, as well as a trending toward urbanization, that poses significant environmental and societal concerns. To manage these concerns, municipal decision-makers are attempting to leverage the Smart City concept with collaboration between external actors as a means to maintain the prepossessed living standard in the city.

In a 2017 paper, Pierce and Andersson, researchers at Lund University in Sweden, developed a framework[44] based on existing literature centered on the predominant challenges in Smart City initiatives. They tested its validity via interviews with municipal decision-makers in mid-sized European cities, i.e., between 100,000 and 600,000 citizens. The results show that municipal decision-makers are mainly concerned with the challenges of non-technical issues such as collaboration, economics, governance and awareness of technology – however, "surprisingly", security is not always perceived as a challenge.

Recognizing this gap, a number of municipal and local government-related groups (e.g. Internal City Management Association (ICMA), National Association of Counties (NaCo)) have indicated that security issues should be of critical importance. In fact, the National Association of Regional Councils (NARC) noted:

> *"To ensure that local governments are able to use computer technology safely and securely, these organizations will need to prioritize security concerns. Strengthening security systems and implementing security best practices in conjunction with new information technology is a crucial step for local governments seeking to take advantage of computer technology, while at the same time protecting the integrity of their systems. Security best practices, as reported by ICMA, include monitoring networks for suspicious activity, creating incident response plans in advance, and installing effective antivirus software."*[45]

[44] Pierce, P., & Andersson, B. (January 2017), "Challenges with Smart Cities initiatives–A municipal decision makers' perspective," *Proceedings of the 50th Hawaii International Conference on System Sciences*. http://scholarspace.manoa.hawaii.edu/handle/10125/41495. The authors describe their initial framework as follows: "based on the literature review two major areas surfaced that was labelled as *non-technical challenges* and *technical challenges*. In the non-technical subset, the following aspects belong: *collaboration, financial, governance, contextual* and *political*. In the technical subset following aspects belong: *privacy, security* and *interoperability*." Following their findings, they revisited their framework and in the non-technical challenges, *contextual* and *political* were replaced by *awareness*; and in the technical subset, *security* was removed. The surprising lack of concern for security needs to be compared with some of the findings of the 2017 Pew Research Center canvassing study on IoT: *"Despite wide concern about cyberattacks, outages and privacy violations, most experts believe the Internet of Things will continue to expand successfully the next few years, tying machines to machines and linking people to valuable resources, services and opportunities,"* Lee Rainie and Janna Anderson, "The Internet of Things Connectivity Binge: What Are the Implications?" June 6, 2017 http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/

[45] NARC (2015) "Digital Woes: The Challenges that Local Governments Face in the Digital Age." http://narc.org/wp-content/uploads/Blog_Local-Government-IT_2015.pdf

In addition to productivity gains focused on effectiveness and efficiency, municipalities can harness IoT technologies, including data collection and analysis, to facilitate (secure) citizen experiences.

Devising novel ways of providing interfaces for citizens and other users of city services with secure[46] backend connectivity and big data analytics that safeguard privacy is an absolute necessity.

2.4.2 Utilities

Water, Waste, Smart Electric Grid

A key characteristic of IoT is that it can provide linkage of the physical world to the internet. The extant model of utilities operation has been based on now-aging electromechanical systems that tended to be designed based on the need to anticipate a wide range of possible conditions, and hence are fairly immutable once in place. System operation was primarily manual and relatively labor intensive.

IoT offers utilities real-time feedback capabilities to better understand the customer needs and perform adjustments to improve the level of service. With appropriately designed IoT, and applicably designed systems, utility networks can be made more secure, reliable, resilient, and sustainable. Given the complexity of maintaining IoT systems with so many discreet components, challenges to deployment include sensing and sensor placement, power management, cyber security, system integration and interoperability, and wireless and cloud connectivity.[47]

In the face of ever-changing and evolving technologies, planning for municipal IoT implementation could benefit from an integrative perspective where collaborative public-private engagement is at the center of all IoT deployment plans and technologies. Public-private-academic partnerships could be sought for mutually beneficial sustainability outcomes; and privacy, security, and interoperability concerns are balanced with trust and reliability. Further, technologies, data, and insights are shared across sectors and with the public, to the extent advisable for confidentiality reasons and security concerns.[48] Utilities must do more than just enhance efficiency—they must also be adaptable/reconfigurable to address frequent and severe weather events; physical security threats; competitive retail

[46] An original perspective on the City of Atlanta's 2018 security breach is provided by Georgia Tech Professor Ian Bogost in "One of the Biggest and Most Boring Cyberattacks Against an American City Yet - A recent ransomware attack on Atlanta's computer systems is disruptive, but so ordinary," The Atlantic, March 28, 2018, https://www.theatlantic.com/technology/archive/2018/03/atlantas-boring-ransomware-attack/556673/

[47] Bedi, G., Venayagamoorthy, G. K., & Singh, R. (2016). Navigating the challenges of Internet of Things (IoT) for power and energy systems. In *Power Systems Conference* (PSC), 2016 Clemson University (pp. 1-5). IEEE https://ieeexplore.ieee.org/document/7462853/

[48] Nonnecke, B. M., Bruch, M., & Crittenden, C. (2016). *IoT & Sustainability: Practice, Policy and Promise.* Center for Information Technology Research in the Interest of Society & the Banatao Institute, University of California. http://citris-uc.org/wp-content/uploads/2016/07/CITRIS_IoT-and-Sustainability-White-Paper.pdf

markets; electric vehicles; the emergence of distributed, nonutility energy generation, storage, and management systems; and the advent of microgrids.[49]

Deployment of smart, connected sensors, and intelligent integrative systems based on streams of sensor-collected data, can provide the backend of more efficient, responsive systems. More broadly, IoT can use data and sensors to bridge a gap between urban infrastructure and smart buildings with tremendous efficiency as well as management impacts. These data applications can also extend into relatively traditional, labor-intensive applications such as waste management and disposal.[50] [51]

As an example, the smart grid network infrastructure deployed by an electric utility is one that can be shared with the municipality for traffic, street lighting, and parking. This can be achieved by extending the smart grid network infrastructure rather than investing in an alternative duplicative network infrastructure. To aid these economies of deployment, regulatory bodies and policies could create a framework that promotes the collaboration between the organizations. The consequential ROI benefits could be passed back to society for further improving the public/social infrastructure.

One current example of IoT usage for utilities includes Berkeley County (S.C.), which deployed sensors and automated reading capabilities to remotely monitor water meters. This resulted in labor-saving efficiencies in terms of managing staff, but of greater strategic value was the ability to get insights into water usage patterns and better allocate resources, as well as the ability to notify customers and service personnel about service leaks.[52]

2.4.3 Public Safety

Public Care, Safe City, Amenity Services (Fire, Police)

This use case can be developed along several dimensions depending on the end application. A key consideration in designing and implementing these (public safety) services is that cities are building a system of systems (SoS), composed of large heterogeneous and independent systems that leverage emergent behavior from their

[49] Collier, S. E. (2015). Smart Grid Apps Must Work Together to Work at All. *Natural Gas & Electricity*, 32(1), 25-28 https://onlinelibrary.wiley.com/doi/full/10.1002/gas.21847

[50] Anagnostopoulos, T., Zaslavsky, A., & Medvedev, A. (2015, April). Robust waste collection exploiting cost efficiency of IoT potentiality in Smart Cities. In *Recent Advances in Internet of Things (RIoT), 2015 International Conference on* (pp. 1-6). *IEEE* *https://www.computer.org/csdl/proceedings/riot/2015/8325/00/07104901-abs.html*

[51] Kale, P. P., Salunkhe, S. R., Dhole, S. B., & Bansode, V. V. (May 2017). Analysis on Smart Waste Management System for Smart Cities using IoT. *International Research Journal of Engineering and Technology (IRJET)*, 4(05) https://www.scribd.com/document/360036854/Analysis-on-Smart-Waste-Management-System-for-Smart-Cities-using-IoT

[52]Sensus Case Study http://na.smartcitiescouncil.com/system/tdf/main/public_resources/Berkeley%20County%20Case%20Study_Final_0.pdf?file=1&type=node&id=4087

interaction. Specialized engineering and design focus on the needs of vulnerable populations is required to build a robust system of systems.[53]

The development of the FirstNet infrastructure provides a connected infrastructure that can be used to support IoT devices. Aside from the ability of IoT to provide robust network services, sensors and devices specifically at the individual level offer promising potential. Public safety responders equipped with IoT-based devices will be able to use data flowing between on-site responders and command centers to generate information about an event scene or intervention status and provide information-based support for critical decisions.[54] Such devices can serve several purposes: providing location-based information on first responders and allowing better decision-making, as well as alerting functions and information that can advise first responders.

Additional novel uses include wearable sensors for vulnerable populations combined with support software that allows first responders to be aware of the existence and needs of people with disabilities and the elderly. It could also serve as potential communication assistance with language barriers.[55] Privacy is a key concern since this sort of data collection could inadvertently reveal characteristics that individuals would prefer kept private.

2.4.4 Transportation

Traffic, Lighting, Parking, Safety

Much of the IoT work related to this use case involves deployment of sensors to collect data to provide better control and management of resources in complex systems.

San Diego, CA has started using cameras built into connected streetlights to monitor pedestrian traffic and reroute cars during peak hours to avoid pedestrian accidents and alleviate congestion, and it has deployed an intelligent network citywide in an effort to optimize traffic and parking, and facilitate better energy management[56].

[53] "*Vulnerable populations include the economically disadvantaged, racial and ethnic minorities, the uninsured, low-income children, the elderly, the homeless, those with human immunodeficiency virus (HIV), and those with other chronic health conditions, including severe mental illness,"* The American Journal of Managed Care, "Vulnerable Populations: Who Are They?, November 1, 2006 http://www.ajmc.com/journals/supplement/2006/2006-11-vol12-n13suppl/nov06-2390ps348-s352. Public safety and emergency alert technological issues are addressed in papers available at the digital library of the Strategic Engineering Institute at Carnegie Mellon University https://resources.sei.cmu.edu/library/

[54] Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Communications Magazine*, 54(4), 47-53 https://ieeexplore.ieee.org/document/7452265/

[55] Wireless RERC. (2017). "Accessibility, Usability, and the Design of Wearables and Wirelessly Connected Devices" (Research Brief #17-01) http://www.wirelessrerc.gatech.edu/sites/default/files/publications/research_brief_accessibility_usability_and_the_design_of_wearables_and_wirelessly_connected_devices_0.pdf

[56] Sameer Sharma, "Smart City Era Promises Big Improvement for Urban Ecosystems," IoT@ Intel blog, June 19, 2018 https://blogs.intel.com/iot/2018/06/19/smart-city-era-promises-big-improvement-for-urban-ecosystems/

San Antonio, TX has implemented use of streetlights that are adjusted in stormy weather to improve visibility and reduce accidents.

Another example is a partnership between Georgia Power and the City of Atlanta, GA to test deployment of a new IoT sensor platform for cities, which includes installation of 1,000 wirelessly controlled LED lights. As part of the Smart Cities pilot, the companies will test these intelligent technologies to help the city make improvements in three key focus areas: mobility (reduced traffic congestion), public safety (improved response time) and the environment (reduced emissions).

More broadly, researchers in Chicago, IL (the Urban Center for Computation and Data of the Computation Institute, a joint initiative of Argonne National Laboratory and the University of Chicago) have set up the "Array of Things" urban sensing project, a network of interactive, modular sensor boxes that will be installed around Chicago to collect real-time data on the city's environment, infrastructure, and activity for research and public use.

2.4.5 Healthcare

Hospitals, Home Care, Emergency Services

Internet of Things technologies will improve the operational efficiency of hospitals and other healthcare facilities and, through telehealth, telemedicine and telecare, enable healthcare providers to optimize the use of their resources. IoT will also change the lives of people with disabilities and senior citizens by giving them access to direct assistance and support, thereby fostering their independence.

The U.S. Federal Communications Commission (FCC) observes that advances in information and communications technologies will allow medical professionals and other "health and care" providers to offer robust, remote (from their location to another), interactive services to patients and caregivers, and provides the following definitions:[57]

> ***"Telemedicine?*** *- Telemedicine can be defined as using telecommunications technologies to support the delivery of all kinds of medical, diagnostic and treatment-related services usually by doctors. For example, this includes conducting diagnostic tests, closely monitoring a patient's progress after treatment or therapy and facilitating access to specialists that are not located in the same place as the patient.*
>
> ***Telehealth?*** *- Telehealth is similar to telemedicine but includes a wider variety of remote healthcare services beyond the doctor-patient relationship. It often involves services provided by nurses, pharmacists or social workers, for example, who help with patient health education, social support and medication adherence, and troubleshooting health issues for patients and their caregivers.*

[57] FCC website, "Telehealth, Telemedicine and Telecare: What's What?," https://www.fcc.gov/general/telehealth-telemedicine-and-telecare-whats-what

> ***Telecare?*** *- Telecare generally refers to technology that allows consumers to stay safe and independent in their own homes. For example, telecare may include consumer-oriented health and fitness apps, sensors and tools that connect consumers with family members or other caregivers, exercise tracking tools, digital medication reminder systems or early warning and detection technologies."*

In summary, according to GSMA:

> *"The dense population of cities stresses the provision of healthcare services and can speed up the spread of disease. The IoT can improve the monitoring of the health of a city's population whilst giving emergency services new tools to improve their response times to emergencies. New solutions can help reduce overcrowding in hospitals and healthcare institutions, and improve the lifestyle of people with disabilities and chronic diseases. Furthermore, health providers and city managers are looking for ways to improve preventative measures such as cleanliness and reduce costs and enhance efficiency of an increasing healthcare burden."* [58]

2.5 CONCLUSIONS AND NEXT STEPS

Given the resources required to conceptualize, design and develop IoT for use in Smart Cities, many of the current projects tend to focus on technology-centric, specialized use cases. One benefit of a so-called "big picture" approach is that it captures specific, data-driven solutions with the social, economic, policy and contextual perspectives which can often be overlooked when municipalities are "in the trenches" while bringing projects online.

An effective way to ensure inclusive projects actually meet the needs of citizens would be to obtain ongoing public input in a way that is equivalent to "design charrettes"[59]. This could be done both online and in-person and would involve end users exploring the range of options and outcomes that could be expected from the implementation of large scale, municipal social/physical IoT infrastructure projects. Examples include collaborative modeling exercises[60], framework foresight[61], and collaborative policy design.[62]

Additionally, in order to achieve a higher ROI, various city functions as well as interest organizations (e.g. municipal services, utilities, transportation, etc.) that come under the

[58] GSMA, "Smart Cities Health," https://www.gsma.com/iot/smart-cities-resources/smart-cities-health/

[59] "*A charette (pronounced "shuh-ret") is an intense period of design activity. In fields of design such as architecture, landscape architecture, industrial design, interior design and graphic design, the term charette may refer to an intense period of work by one person or a group of people prior to a deadline. The period of a charette typically involves a focused and sustained effort."* Source: Ashley Bland, "What is a Design Charette,", Travois Website, https://travois.com/design-charette/

[60] Turoff, M., Bañuls, V. A., Plotnick, L., Hiltz, S. R., & de la Huerga, M. R. (2016). A collaborative dynamic scenario model for the interaction of critical infrastructures. *Futures*, 84, 23-42 https://www.infona.pl/resource/bwmeta1.element.elsevier-5d121c6e-854a-3dc7-8c97-ad65b58ee850

[61] Hines, A. & Bishop, P. C. (2013). Framework foresight: Exploring futures the Houston way. *Futures,* 51, 31-49 http://www.andyhinesight.com/wp-content/uploads/2016/03/93-Framework-Foresight.pdf

[62] Gandy, M., Baker, P. M., & Zeagler, C. (2017). Imagining futures: A collaborative policy/device design for wearable computing. *Futures*, 87, 106-121 https://www.infona.pl/resource/bwmeta1.element.elsevier-922f5cd0-efa9-3849-a0a6-3196b0ef9af9

Smart City umbrella should collaborate to invest in a shared network canopy and enterprise infrastructure wherever possible. This could include, for instance: developing a consolidated plan for investment in network and enterprise infrastructure(s) with a combined ROI model; or a cost-sharing model (capex, deployment costs, operations & maintenance costs).

With a "system of systems" perspective, a Smart City's design should allow for a network supporting many functions and internal members with various bandwidth and quality of service requirements; enterprise cloud service sharing; and smart data exchange for near real-time data analytics.

Addressing policy impact after the fact, rather than as projects are being rationalized and developed, runs the risk of generating unanticipated consequences, including costly failure situations, which could doom future innovations before they leave the drawing board.

Engagement from all citizens, especially those most vulnerable is critical:

> *"Re-incorporating the voices of ordinary citizens – including the poor ones, the inhabitants of the slums of the Global South, and other technologically marginal or even subaltern subjects – means finding a credible way of imagining a nexus between citizens and urban technologies that is truly empowering and respectful of citizens' wishes and hopes."*[63]

As noted in a Demos Helsinki report, "The Internet of Things is not about technology, it's about society." [64]

[63] Vanolo, A. (2016), "Is there anybody out there? The place and role of citizens in tomorrow's Smart Cities," *Futures*, *82*, 26-36 https://www.sciencedirect.com/science/article/pii/S0016328716300301

[64] http://www.demoshelsinki.fi/en/2015/11/12/the-internet-of-things-is-not-about-technology-its-about-society/

3 QUESTION 2: DATA OWNERSHIP AND IOT SECURITY

WHAT ARE THE DATA OWNERSHIP AND SECURITY ISSUES, AND HOW WILL THEY BE ADDRESSED?

3.1 INTRODUCTION

In 1933, the Tennessee Valley Authority (TVA) was created to modernize very poor regions by building dams and reservoirs that generated electricity to power the growth of an entire region. In addition to creating a reliable source of energy, the massive infrastructure overhaul enabled the scientific, technological, and manufacturing advancements created through Oak Ridge National Labs, the Manhattan Project, and Alcoa that contributed to broader national security and economic interests. Accomplishing this feat required the TVA to work with multiple federal agencies, universities, state governments, and private industries.

While the collaborative efforts of TVA are notable, regions now face a similar societal shift as they seek to modernize infrastructure and evolve from disparate municipal organizations into connected Smart Cities. These transformations also have societal impacts with respect to privacy and secure communications as noted by the 1973 U.S. Secretary of Health, Education, and Welfare privacy report (HEW Report):

> *"An agrarian, frontier society undoubtedly permitted much less personal privacy than a modern urban society, and a small rural town today still permits less than a big city. The poet, the novelist, and the social scientist tell us, each in his own way, that the life of a small-town man, woman, or family is an open book compared to the more anonymous existence of urban dwellers."*[65]

While this report was concerned with the lack of privacy in rural areas, the societal impact of infrastructure modernization is magnified in a Smart City as interconnected ecosystems create systemic benefits and risks. As such, technology adoption is dependent upon the stakeholders' trust that the data generated and exchanged will be secured and their privacy not violated. Data security in this context is not confined to the technical challenges that arise with the proliferation of sensors and enhanced data transmission capabilities, but includes privacy implications when data shared between multiple parties is breached.

Security frameworks extend beyond people-centric use cases. Ensuring that robust, resilient security infrastructure and protocols are in place to protect the estimated 20 billion things that will connect to the internet is a tremendous challenge. Using the Product Onion model presented by Khan et al. (Figure 4)[66], cities can use role-based access policies to support end-to-end application security as participants more freely transition between traditional functions.

[65] Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Educ., & Welfare, "Records, Computers, and the Rights of Citizens", 29–30 (1973) [hereinafter HEW Report] available at https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[66] Z. Khan, Z. Pervez, A.G. Abbasi, *Towards a secure service provisioning framework in a Smart City environment, Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.06.031

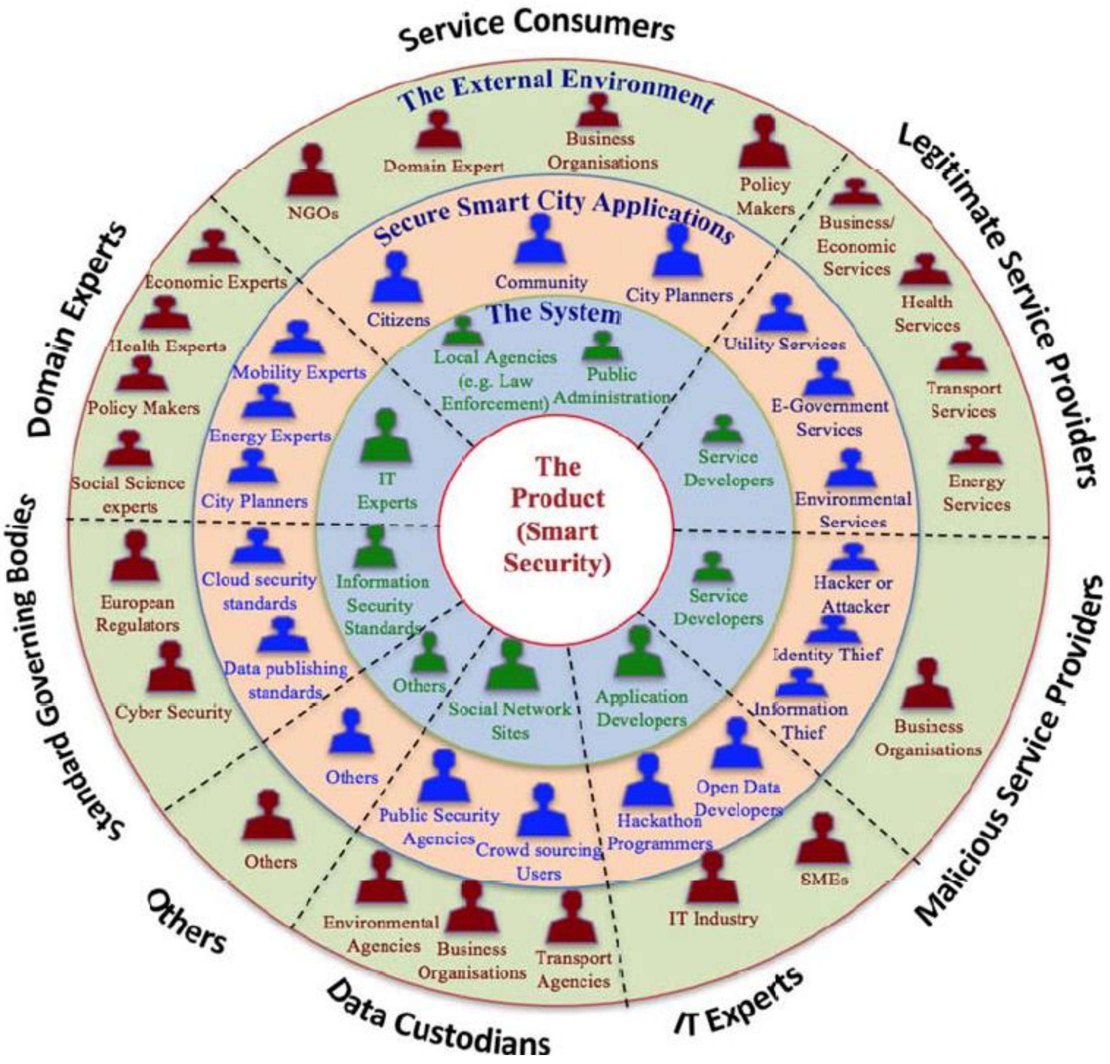


Figure 4: The Product Onion Model.[67]

These newly connected stakeholders also serve as new attack vectors, which are not fully addressed using traditional data security and privacy practices. Network vulnerabilities that were previously isolated to one participant could be exploited and potentially pose a systemic threat to related stakeholders. As Zhang et. al. point out,

> *"Although some off-the-shelf techniques (encryption, authentication, anonymity, etc.) and policies might be directly applied to avert these problems, the emerging "smart" attackers could still infer and violate privacy in many other ways, such as side channel attack and cold boot attack. Without sufficient security and privacy protections, users may refrain from accepting the Smart City, which would remain as a far-off futuristic idea."*[68]

[67] Source: Z. Khan, Z. Pervez, A.G. Abbasi, *Towards a secure service provisioning framework in a Smart City environment, Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.06.031

[68] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. and Shen, X. (2017). *Security and Privacy in Smart City Applications: Challenges and Solutions*. IEEE Communications Magazine, 55(1), pp.122-129.

3.2 IoT Security

As should be abundantly clear by now, no reflection on the future of smart cities can overlook the foundational importance of security.[69] The Internet of Things has introduced new security risks, which represent significant hurdles for device and software engineers.

The way we routinely function in a growingly digital society must be thoroughly scrutinized with security in mind. As a case in point, research conducted by Professors Milos Prvulovic and Alenka Zajic at Georgia Tech reveals not only that side-channel attacks extract data values (such as cryptographic keys), but also that electromagnetic (EM) emissions from modern systems (computers, sensors, IoT devices) can leak sensitive information and be detected from several meters away. This information can be used to learn more about program behavior as current flows in the systems can vary with program activity.

> *"The issue: In the same way clicking keyboard sounds could give indications of what a person is typing, a machine emits frequency waves that provides (sic) much better tips. That means a "Russian radio" antenna taped underneath a desk, for instance, can detect what a person is doing on a laptop that isn't plugged in, connected to the internet, or wirelessly communicating. Such "side channel" attacks have helped researchers copy the key fobs of modern cars or eavesdrop on encrypted VoIP calls."* [70]

IoT devices often have few resources that can be leveraged to monitor their security, and they often have limited hardware and system support for isolation and protection. These limitations make existing malware detection techniques inadequate as they require significant computation power and resources on the monitored device itself.[71] Dr. Prvulovic's team has demonstrated a new method to detect malware by externally observing EM signals by an IoT system that was effective against a number of malicious activities such as control-flow hijacking, Mirai botnet, and ransomware.[72]

[69] See for example: "Cybersecurity is a prerequisite for the smart city, argued Gadi Mergi, CTO at Israel's National Cyber Directorate," in Gil Press, *6 Ways To Make Smart Cities Future-Proof Cybersecurity Cities,* Forbes, February 14, 2018, https://www.forbes.com/sites/gilpress/2018/02/14/6-ways-to-make-smart-cities-future-proof-cybersecurity-cities/#6fbe302b4240; and Skip Descant, *NIST Global City Teams Challenge to Focus on IoT Security in Smart Cities,* FutureStructure, January 23, 2018, http://www.govtech.com/fs/infrastructure/NIST-Global-City-Teams-Challenge-to-Focus-on-IoT-Security-in-Smart-Cities.html

[70] Sean Sposito, *Computer 'Emissions' Raise Privacy Worries*, AJC, April 27, 2015, https://www.myajc.com/business/computer-emissions-raise-privacy-worries/5nW60lEsdqCga47qAWepCI/

[71] Sehatbakhsh, N., Nazari, A., Zajic, A. and Prvulovic, M. (2016). Spectral profiling: Observer-effect-free profiling by monitoring EM emanations. *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, http://alenka.ece.gatech.edu/wp-content/uploads/sites/463/2016/08/MICRO16.pdf

[72] See, for example, Nader Sehatbakhsh et al., *Leveraging Electromagnetic Emanations for IoT Security* (May 2017) https://www.cc.gatech.edu/~milos/Papers/2017_HOSTDemo.pdf

More generally, stakeholders must continuously evaluate and implement tight risk (including uncertainty) management safeguards as IoT systems and applications are designed, tested, deployed and maintained across both legacy and new systems[73].

While the IoT landscape is still fragmented (a challenge that should not be underestimated), substantial progress on the standardization front has been made in the last few years. Remarkable work is taking place in both the United States and the European Union to assess the extent and depth of the current state of international cybersecurity standards development for IoT as exemplified by the two following reports:

- U.S. National Institute of Standards and Technology (NIST), Department of Commerce, “Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT),” Draft NISTIR 8200, February 2018 (see in particular Section 8 - Standards Landscape for IoT Cybersecurity, and Annex D – IoT Standards Mapping to Core Areas of Cybersecurity)[74]

- European Union Agency for Network And Information Security (ENISA), “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,” November 2017 (see in particular Annex C: Security Standards and References Reviewed)[75]

Cities can utilize architectures, frameworks, protocols, standards, guidelines, and best practices for IoT security (and privacy) that have been (and continue to be) developed by a wide range of alliances, consortia, fora, government bodies, and regulatory authorities. These organizations include (without any claim to exhaustiveness):

[73] The Cyber-Physical Systems Public Working Group (CPS PWG) established by the National Institute for Standards and Technology (NIST) identifies five top-level trustworthiness properties of [IoT] systems that risk managers should consider when performing risk management: cybersecurity (or security); privacy; safety; reliability; and resilience - see NIST Special Publication 1500-202 Framework for Cyber-Physical Systems: Volume 2, Working Group Reports, Version 1.0, June 2017, p.15 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf. Note that resilience, i.e., the ability *“to address uncertainty, situations where the distribution of possible outcomes produced by the interaction of the system with its environment are NOT known, often because the environment conditions that produce the impacts are unknown or not well understood,”* is viewed in the NIST framework as *“perhaps the most significant challenge”* (p. 4) – see also Louchez, A. & Rosner, G. (April14, 2016), Internet of Things Security: The Case for Systemic Resilience in *Sensors Magazine* https://sensorsmag.com/iot-wireless/internet-things-security-case-for-sytemic-resilience

[74] Available at https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf. The report was produced by the U.S.-based Interagency International Cybersecurity Standardization Working Group (IICS WG), which was established in December 2015 by the National Security Council’s Cyber Interagency Policy Committee (NSC Cyber IPC). Its purpose is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization.

[75] Available at https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.. ENISA was created in 2004 by EU Regulation No 460/2004 under the name of European Network and Information Security Agency. The Agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the [European Union] internal market

- 3rd Generation Partnership Project (3GPP)
- Alliance for Internet of Things Innovation (AIOTI)
- Alliance for Telecommunications Industry Solutions (ATIS) - Smart Cities – Technology Roadmap (2017) and Data Sharing Framework for Smart Cities (March 2018)
- Alliance of Industrial Internet (China) – Industrial Internet Architecture – Version 1.0 (2016)
- Broadband Forum
- Atlantic Council (Brent Scowcroft Center on International Security) – Smart Homes and the Internet of Things Issue Brief (March 2016)
- Body of European Regulators for Electronic Communications (BEREC) – Report on Enabling the Internet of Things (February 2016)
- Broadband Internet Technical Advisory Group (BITAG) (IoT Security and Privacy Recommendations)
- BuildItSecure.ly
- CableLabs (A Vision for Secure IoT – Summer 2017)
- Center for Internet Security (CIS) - Internet of Things Security Companion to the CIS Critical Security Controls (Version 6) White Paper (posted on August 2016)
- Cloud Security Alliance (IoT Working Group)
- Cloud Standards Customer Council (CSCC) – Cloud Customer Architecture for IoT (2016)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Common Criteria
- CompTIA - CompTIA Channel Standard for Cybersecurity, and Sizing Up the Internet of Things White Paper (August 2015)
- Computer Science and Telecommunications Board (CSTB cybersecurity and trustworthiness projects)
- Computing Community Consortium (CCC) - Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things White Paper (February 2017)
- CTIA (the Wireless Association) – Protecting America's Wireless Networks White Paper (2017)
- DASH7 Alliance
- Digital Standard (The)
- DTSec (DTS Cybersecurity Standard for Connected Diabetes Device Security and DTS Protection Profile for Connected Diabetes Devices)
- Eclipse (Eclipse ioFog)
- Electricity Information Sharing and Analysis Center (E-ISAC) – Internet of things DDoS White Paper (October 2016)
- EnOcean Alliance
- Euralarm – Smart Cities: Revolution in every area of life White Paper (November 2016)
- European Telecommunications Standards Institute (ETSI) (Roles and Activities in Security)
- European Union (several horizontal and vertical initiatives, including European General Data Protection Regulation (GDPR) and the European Research Cluster on the Internet of Things (IERC))
- European Union Agency for Network and Information Security (ENISA) – Baseline Security Recommendations for IoT in the context of critical information infrastructures (November 2017)
- EuroSmart - Eurosmart: Internet of Trust, Security and Privacy in the connected world Position Paper (November 2016) and Making Europe's Smart Cities, safe, secure White Paper (February 2015)
- Fairhair Alliance – Facilitating the Internet of Things For Commercial Buildings White Paper (2017)
- FIDO Alliance
- Fraunhofer (Germany) - FOKUS and Institute for Integrated Circuits (IoT-Bus – The Secure Communication Bus)
- Georgia Tech Institute for Information Security and Privacy (IISP)
- Georgia Tech Institute for People and Technology (IPaT Research)
- Global Cyber Alliance (Smart Cities and IoT)
- Global Platform - Industrial Internet of Things Taskforce [f.k.a. Internet of Things Taskforce] and Consumer IoT Task Force [f.k.a. Mobile Task Force]
- Global Semiconductor Alliance (GSA) – Security in the IoT White Paper (2017)
- GS1 (GS1 and the Internet of Things – October 2016)
- GSMA (IoT Security Guidelines and Smart Cities Safety)
- HITRUST Alliance
- HL7 Standards
- Hypercat (Global Alliance and standard (PAS 212) driving secure and interoperable Internet of Things (IoT) for Industry and cities)
- Industrial Internet Consortium (IIC) (Security Framework, October 2016)
- Information Security and Privacy Advisory Board (ISPAB)

- Information Technology Industry Council (ITI)
- INRIA (France) (cybersecurity)
- Institute for Critical Infrastructure Technology (ICIT) - Publications
- Institute of Electrical and Electronics Engineers (IEEE): IEEE Internet of Things initiative and IEEE Smart Cities
- Interagency International Cybersecurity Standardization Working Group (IICS WG), "Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)", February 2018, Draft NISTIR 8200
- InterNational Committee for Information Technology Standards (INCITS) (Ad Hoc on IoT Security and Privacy)
- International Electrotechnical Commission (IEC) (IoT 2020: Smart and Secure IoT Platform) ISO/IEC JTC 1 (Internet of Things and Related Technologies) (ISO/IEC CD 30141 – IoT RA)
- International Interconnection Forum for Services over IP (i3Forum) – Internet of Things White Paper – Release 1.0 (2017)
- International Organization for Standardization (ISO) (related standards: ISO/IEC 27001:2013; ISO/IEC 27002:2013; and ISO/IEC 27031:2011)
- International Telecommunication Union (ITU) (ITU-T Study Group 20 and ITU-T Study Group 13)
- International Society of Automation (ISA) (Industrial Automation and Control System Security (ISA99))
- Internet Architecture Board (IAB) - Internet of Things Software Update Workshop (IoTSU) 2016
- Internet Engineering Task Force (IETF) - Rough Guide to IETF 100: The Internet of Things; Best Current Practices for Securing Internet of Things (IoT) Devices; and State-of-the-Art and Challenges for the Internet of Things Security
- Internet of Things Alliance (presentations from securing your IoT data event)
- Internet of Things Consortium (IoTC)
- Internet of Things Privacy Forum (IoTPF)
- Internet Society (Policy Brief – October 2016)
- IoT Alliance Australia (IoT Security Guideline, February 2017)
- IoT Cybersecurity Alliance (IoTCA)
- IoT Security Foundation – Establishing Principles for IoT Security Guide (2016)
- IPSO Alliance [now OMA SpecWorks] – Security, Privacy and Identity Working Group (launched in 2017)
- ISACA (Internet of Things: Risk and Value Considerations) – ISACA Journal, The Internet of Things, volume 3, 2017
- Linux Foundation's Hyperledger open source collaborative effort
- LoRa Alliance (LoRa WAN Security)
- National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (Japan) (General Framework for Secured IoT Systems, August 2016)
- National Institute of Standards and Technology (NIST) (NIST initiatives IoT, Information Technology Laboratory, Applied Cybersecurity Division)
- National Security Telecommunications Advisory Committee (NSTAC) (NTASC Report to the President on the Internet of Things, 2014)
- National Telecommunications and Information Administration (NTIA) (Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching)
- New Zealand IoT Alliance (IoT Cybersecurity, and IoT Data and Privacy Working Groups)
- North American Electric Reliability Corp. (NERC) - NERC cybersecurity standard
- OASIS (Cyber Standards Council)
- Object Management Group (see IIC) (OMG cybersecurity initiatives)
- oneM2M (Published Specifications)
- Online Trust Alliance (IoT Trust Framework, January 2017)
- OPC Foundation (Security info: bulletins, recommendations and analysist)
- Open Connectivity Foundation (OCF Security)
- Open Geospatial Consortium (OGC) (Security Working Group)
- Open Group Internet of Things (IoT) Work Group
- Open Mobile Alliance (OMA) [now OMA SpecWorks] (OMA Application Layer Security Common Functions Overview)
- Open Standard for Public Transport (OSPT) (CIPURSE™ open security standard)
- Open Web Application Security Project (OWASP)
- OpenFog Consortium (OpenFog Reference Architecture for Fog Computing, February 2017)
- OSGi Internet of Things Expert Group (IOTEG)

- Personal Connected Health Alliance – Global Policy Priorities (Winter 2017)
- Platform Industrie 4.0 (Germany) – Security in RAMI 4.0 (RAMI = Reference Architecture Model for Industrie 4.0)
- SAE International (Vehicle Electrical System Security Committee)
- SANS Institute (Reading Room – IoT Papers)
- Secure Smart and Resilient Cities Initiative (SSCI)
- Secure Technology Alliance [f.k.a. Smart Card Alliance] (Internet of Things Security Council) and Embedded Hardware Security for IoT Applications White Paper (2016) and Blockchain and Smart Card Technology (2017) White Paper
- Securing Smart Cities ("Let's make smart cities cyber-safe") – Also guidelines for Smart Technology Adoption jointly developed by Securing Smart Cities and the Cloud Security Alliance (CSA) (November 2015)
- Smart Cities Council (Security and Privacy Website Section)
- Smart Electric Power Alliance (catalog of standards)
- Telecommunications Industry Association (TIA) – TR-48 | Vehicular Telematics; TR-50 | M2M -Smart Device Communications; TR-51 | Smart Utility Networks
- Thread Group Security & Commissioning [pdf]) (July 2015)
- Trusted IoT Alliance ("leveraging blockchain infrastructure to secure and scale IoT ecosystems")
- Trusting Computing Group (IoT Work Group)
- The Update Framework (TUF)
- Underwriters Laboratories (UL) (UL Cybersecurity Assurance Program)
- United Kingdom Department of Digital, Culture, Media and Sport (DCMS) - Security by Design report on improving the cyber security of consumer Internet of Things (March 2018)
- United Kingdom IoT-related initiatives: Digital Catapult, Future Cities Catapult, IoTUK and PETRAS
- UK PETRAS IoT Hub - Summary literature review of industry recommendations and international developments on IoT security (2018)
- U.S. CERT (ST17-001 – Securing the Internet of Things)
- U.S. Chamber of Commerce Principles for IoT Security, September 2017, and IoT Cyber Policy, October 19, 2017
- U.S. Department of Commerce (Green Paper: Fostering the Advancement of the Internet of Things, January 2017)
- U.S. Department of Homeland Security (DHS) - Strategic Principles for Securing the Internet of Things, November 2016, and also DHS S&T [Science and Technology Directorate]-NIST "Smart and Secure Cities and Communities Challenge" (SC3)
- U.S. Department of Transportation (National Highway Traffic Safety Administration (NHTSA)) (Cybersecurity Best Practices for Modern Vehicles, October 2016)
- U.S. Federal Communications Commission (FCC) (Cybersecurity Risk Reduction – January 2017)
- U.S. Federal Trade Commission (FTC) (FTC Staff Report - Internet of Things: Privacy and Security in a Connected World) (January 2015)
- U.S. Food and Drug Administration (FDA) (Cybersecurity)
- U.S. Government Accounting Office (GAO) (Internet of Things: Status and Implications of an Increasingly Connected World)
- US Ignite
- Weightless SIG - Security
- Wilson Center (Urban Sustainability Laboratory Research) (Part 1: When Smart Cities Become Digitally Insecure; Part 2: Smart Cities Face a Dynamic Cybersecurity Landscape; and Part 3: Protecting our Cities from Cyber Attacks)
- Wi-SUN Alliance - The Rise of the Internet of Things (2017)
- World's Smart Cities Organization - WCSO
- World Smart City (partnership between IEC, ISO and ITU)
- World Wide Web Consortium (W3C) – Tackling Data Security and Privacy Challenges for the Internet of Things presentation (2016); Web of Things Interest Group; Web of Things Working Group (launched in early 2017); and Web of Things Security and Privacy Considerations (2017)
- Zigbee Alliance – Zigbee: Securing the Wireless IoT White Paper (Q1 2017)
- Z-Wave Alliance

In addition to these organizations, the Security and Privacy Working Group[76] of CDAIT is also developing security- and privacy-related information to help companies and organizations that are building and deploying connected environments.

3.3 USE CASES

Whether the device is a smart energy meter, a parking meter, a pressure valve, or an environmental sensor, all of these devices require at least some level of onboarding, management, and data security. As the asset classification and primary tasks become more critical, the required data security model protecting the system of systems that consume this data, and in some cases provide Supervisory Control and Data Acquisition (SCADA) functionality, must be implemented with an interoperable, standards-based approach.

3.3.1 Municipal Services Management

Smart City technologies are intended to improve how municipalities engage with, and deliver services to, their citizens.

In Jakarta, Indonesia, a district of 10 million people is divided into five cities, 44 sub-districts, and 267 villages. The city government receives an average of 1,400 messages per day via its mobile app, which allows users to submit feedback about public services. The city established a centralized data hub for integrating information from the citizen feedback app and social networks, as well as government services such as transportation, healthcare, water distribution and other departments. After analyzing data on the villages with the highest number of complaints, officials found that most of the complaints stemmed from the lack of garbage collection. They were able to work with village leadership and Jakarta Waste Management on the routing and scheduling to significantly improve garbage collection, and subsequently reduced the number of complaints.

The proliferation of connected sensors expands the attack plane and requires the proper security expertise to manage such devices. The Jakarta use case[77] illustrates how Smart Cities can provide enhanced municipal services that utilize public feedback mechanisms, while mitigating the risk of deploying compromised devices.

[76] At the time of this writing: Dr. Margaret Loper (Georgia Tech) – chair, Peter Allor (Honeywell) – vice-chair, Tim Hahn (IBM) – vice-chair, and Joel Odom (Georgia Tech) – vice-chair.

[77] Details about the Jakarta Smart City (JCS) use case can be found here: https://www.ibm.com/case-studies/jakartasmartcity. Established in 2015 as a management unit under the Communication, Informatics and Statistics division of the Jakarta Provincial Government, Jakarta Smart City has a mission to realize a New Jakarta that is more data-driven and transparent, as well as supporting collaborations through the use of technology for better public services. Its six key focus areas are smart living, smart mobility, smart governance, smart environment, smart economy, and smart people.

3.3.2 Utilities

As the industry adopts IoT and cloud technologies, utilities must enhance security while simplifying compliance. Doing so will allow administrators to focus efforts on improving public and personnel safety and transforming data from the grid into insightful business intelligence.

Energy and grid management applications require much more distributed intelligence to cope with large amounts of data and rapid control response. As IoT introduces millions of devices and latency-sensitive transactions, the traditional cloud-only approach will need complementary capabilities at the edge.

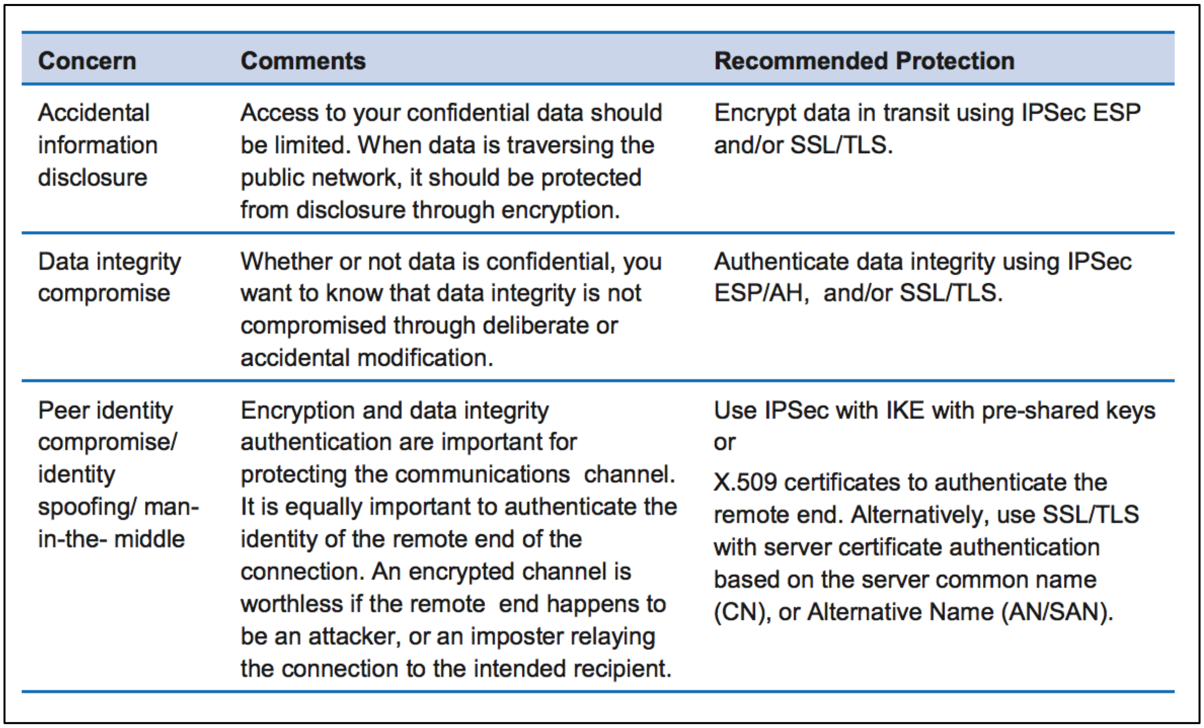
The challenges of data overload and low-latency response can be overcome by edge computing[78]. Edge computing allows applications to execute within the IoT network, providing the intelligence to analyze data locally and generate actions like closing a switch. By giving the gateways and endpoints at the edge the ability to handle computational tasks, organizations reduce the amount of data that needs to be sent to the cloud for processing, analysis and storage.

Utilities need to distribute security across the smart grid by “smartening up” the edge devices to be more security aware and using the network as a sensor and enforcer of security policy. While securing devices at the onset can provide added resiliency, system owners should also consider reliable and cost-effective paths for ongoing and continuous updates, i.e. security patching, firmware updates, etc. on the devices. Cloud-based deployments of IoT solutions allow for devices to be patched or updated remotely, in an automated way, and at scale.

Cloud-based IoT solutions allow for a centralized way for end device on-boarding, authentication, and authorization, as well as secure bi-directional communication with the device. At any given point in time, the customer has the ability to disconnect or disengage one or more devices from a solution if there is a suspicion of threat by simply de-activating security credentials used by device(s) to authenticate with the cloud-based service. This is challenging to accomplish with an on-premises deployment.

IoT applications can communicate over public links, such as the internet, so it is important to protect data in transit. This involves protecting network traffic between endpoints and servers, as well as network traffic between servers. Table 1 below lists common concerns for communication over public links, e.g., the internet, and recommended protection steps to employ.

[78] Various perspectives exist on what edge computing is. See Section 4.3.4 Connectivity (Computing)



Concern	Comments	Recommended Protection
Accidental information disclosure	Access to your confidential data should be limited. When data is traversing the public network, it should be protected from disclosure through encryption.	Encrypt data in transit using IPSec ESP and/or SSL/TLS.
Data integrity compromise	Whether or not data is confidential, you want to know that data integrity is not compromised through deliberate or accidental modification.	Authenticate data integrity using IPSec ESP/AH, and/or SSL/TLS.
Peer identity compromise/ identity spoofing/ man-in-the- middle	Encryption and data integrity authentication are important for protecting the communications channel. It is equally important to authenticate the identity of the remote end of the connection. An encrypted channel is worthless if the remote end happens to be an attacker, or an imposter relaying the connection to the intended recipient.	Use IPSec with IKE with pre-shared keys or X.509 certificates to authenticate the remote end. Alternatively, use SSL/TLS with server certificate authentication based on the server common name (CN), or Alternative Name (AN/SAN).

Table 1: Common Concerns for Communication over Public Links[79]

3.3.3 Public Safety

Like most infrastructure overhauls, Smart City projects involve long-term planning and investment to ensure interoperability among new solutions while replacing legacy systems. In 2013, Miami-Dade County began implementing intelligent services that track water leaks in parks. The solution was designed to alert park managers whenever a leak was detected, minimizing water waste and cutting costs. In addition to saving the county over $1,000,000 in its first year, the solution was able to alert police of incidents where people were stealing valuable copper piping from the municipal sprinkler system.[80] The foundational data hub created by Miami-Dade County enabled substantial public safety and law enforcement advancements by also deploying intelligent video analytics and gunfire detection solutions. In this case, the data hub created by Miami-Dade County ensured that data, which was previously stored in disparate silos, adhered to all applicable data governance and security standards.

3.3.4 Transportation

Recognizing that the modernization of transportation infrastructure is a shared responsibility, stakeholders must implement trusted data-sharing practices between

[79] AWS, *AWS Security Best Practices*, August 2016, https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

[80] See Sarah Rich, *IBM and Miami-Dade County Partner for Smarter Cities Initiative,* Government Technology, March 4, 2013, http://www.govtech.com/e-government/IBM-and-Miami-Dade-County-Partner-for-Smarter-Cities-Initiative.html

municipalities and the private sector to fully realize the benefits of an IoT-enabled infrastructure. As part of the Renew Atlanta Infrastructure bond program, the City of Atlanta partnered with Together for Safer Roads (TSR), a coalition of global private sector companies, to reduce the number of pedestrian and vehicle crashes along the North Avenue smart corridor. In 2014, the crash rate on North Avenue was more than 200 percent worse than the statewide average for similar corridors. To determine the best solutions to reduce this crash rate, and ultimately save lives, the coalition is analyzing hyper-local root causes of collision risk to forecast warning alerts. Analysis is based on curating and aggregating data sources and insights from the City of Atlanta and TSR member companies.[81]

3.3.5 Healthcare

A recent study[82] published in *The American Journal of Managed Care* on data breaches in U.S. hospitals showed that hospital data breaches accounted for approximately 30 percent of large data security incidents reported to the Office of Civil Rights from 2009 to 2016:

> *"Paper and films were the most frequent location of breached data, occurring in 65 hospitals during the study period, whereas network servers were the least common location but their breaches affected the most patients overall."*

The authors recommend that:

> *"Information security systems should be concurrently implemented alongside health information technologies. Improving access control and prioritizing patient privacy will be important steps in minimizing future breaches."*

Given the increasing penetration of IoT technologies in hospitals and their potential vulnerabilities, emphasis on security should be mandatory.

A 2018 report from IoT security company Zingbox, whose researchers detected, identified and analyzed the behavior of medical devices deployed in more than 50 hospitals, clinics, and other healthcare locations, found that:

> *"Many organizations don't have a clear picture of the vulnerabilities on their networks — or even what devices are connected on those networks."*[83]

[81] "Together for Safer Roads Partners With Three Global Cities To Address Critical Road Safety Challenges." Together for Safer Roads, 21 Feb. 2017, www.togetherforsaferroads.org/press/press-release-safer-roads-challenge/.

[82] Meghan Hufstader Gabriel et al. "Data Breach Locations, Types, and Associated Characteristics Among US Hospitals," February 14, 2018 http://www.ajmc.com/journals/issue/2018/2018-vol24-n2/data-breach-locations-types-and-associated-characteristics-among-us-hospitals

[83] Zingbox Press Release, "Groundbreaking Zingbox Report Analyzes Connected Medical Devices Across 50 Locations, Shedding Light on IoT Security Vulnerabilities," March 1, 2018 https://www.zingbox.com/press-releases/groundbreaking-zingbox-threat-report/

The Zingbox survey acknowledged that while infusion pumps make up nearly 50 percent of connected devices in hospitals, they do not represent the largest cyberattack surface (only 2 percent). It is not a reassuring fact: a single breach could have lethal consequences. However, the report provided the following insight, which should point to the next steps for hospital and city managers, i.e., education and training on (IoT) security:

> *"The vast majority of user practice issues stem from employees unaware of sound security practices and not from intentional acts to infect or disable connected medical devices."*[84]

3.4 TRANSPARENCY OF OWNERSHIP

As more aspects of city life become connected and automated, streamlining personal elements such as identity become increasingly important. Being able to digitally verify identity and needed information can provide a positive individual experience and promote security of information. Distributed Ledger Technology (DLT) is one method that can be used to manage personal identities and information.

Distributed Ledger Technologies (DLTs), of which blockchain is the best-known example, can be customized based on the use case but become more useful when utilized as the underlying infrastructure connecting various deployments. DLT can also have the benefits of being immutable and secure while being accessible for authorized parties. A universal identity distributed ledger would enable individuals to manage all of the information about themselves and authorize data access only as needed, promoting privacy.

Benefits for individuals are control, convenience and privacy. Benefits for businesses, governments, and organizations are streamlined applications and secure verifications. By having their personal data on a distributed ledger, an individual could control the access to their information.

When applying for insurance or a mortgage, instead of a lengthy application with copies of documents for verification, the applicant can specify what information should be made available and send an access code to the company. The insurance company accesses the information needed from the ledger and can approve or deny the application.

Figure 5 illustrates how information contributed to the distributed ledger is verified only by trusted members of the ledger such as government, financial institutions, and other entities who have verified the data being populated.

Companies, governments, and organization using the ledger for data and identity verification save significant time and resources in their onboarding and verification processes by trusting that the other members of the ledger have properly verified the information.

[84] Brian Buntz, "Why IoT Security Issues Still Loom Large in Health Care," Internet of Things Institute Website, March 20, 2018 http://www.ioti.com/security/why-iot-security-issues-still-loom-large-health-care

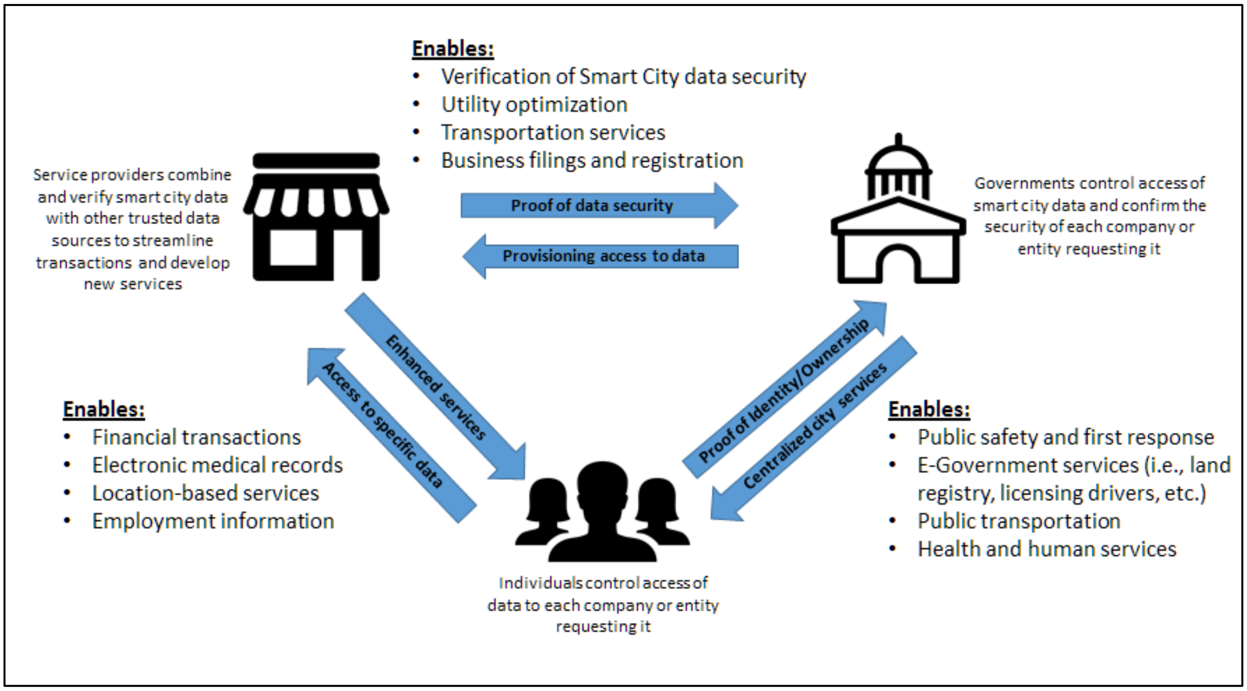

Enables:
Verification of Smart City data security
Utility optimization
Transportation services
Business filings and registration
Service providers combine and verify smart city data with other trusted data sources to streamline transactions and develop new services
Proof of data security
Provisioning access to data
Governments control access of smart city data and confirm the security of each company or entity requesting it
Enhanced services
Access to specific data
Proof of Identity/Ownership
Centralized city services
Enables:
Financial transactions
Electronic medical records
Location-based services
Employment information
Enables:
Public safety and first response
E-Government services (i.e., land registry, licensing drivers, etc.)
Public transportation
Health and human services
Individuals control access of data to each company or entity requesting it

Figure 5: How information contributed to blockchain is verified by trusted members[85]

This concept has been discussed for specific use cases such as interbank applications, healthcare information[86] , insurance[87], or financial requirements for Know Your Customer (KYC) regulations. Because of the all-encompassing nature of this concept, full benefit of an identity blockchain can only be realized once government, companies, and individuals align on the regulatory, security, and privacy elements.

[85] Developed by Forrest Pace (AIG) and Gloria Rismondo (Global Payments) within the CDAIT IoT Thought Leadership Working Group.

[86] See this recent related article: Paul LaBrec, “Healthcare data and blockchain technology,” Inside Angle from 3M Health Information Systems, April 20, 2018, https://www.3mhisinsideangle.com/blog-post/healthcare-data-and-blockchain-technology/

[87] See press release: “AIG, IBM, Standard Chartered Deliver First Multinational Insurance Policy Powered by Blockchain,” Business Wire, June 15, 2017, https://www.businesswire.com/news/home/20170615005586/en/AIG-IBM-Standard-Chartered-Deliver-Multinational-Insurance

3.5 CONCLUSIONS AND NEXT STEPS

Security and privacy are two related but separate issues.

Broadly speaking, security refers to protecting data/information from being improperly accessed/affected while privacy refers to the improper use of data/information (see Section 5.2 on “Privacy as the Cornerstone of Citizen Interaction”).

Smart Cities will have to address both. Security can be especially tricky due to the nature of many IoT devices: limited computing capabilities, limited memory, and extreme power limitations. These challenges make it difficult-to-impossible to implement on-device security measures. Security must therefore be addressed holistically at the system level to ensure the integrity of data.

Scores of security frameworks have been created by reputable organizations seeking to help system implementers. Some are general while some are very industry specific.

The key is for implementers to consider these issues from the beginning. By designing a system to be robust and secure, but with an eye towards the specific use case the system is meant to address, security and privacy can be maximized.

4 QUESTION 3: IoT BUSINESS MODELS

WHAT WILL IoT BUSINESS MODELS LOOK LIKE AND WHAT WOULD CONSTITUTE “SUCCESSES”?

4.1 INTRODUCTION

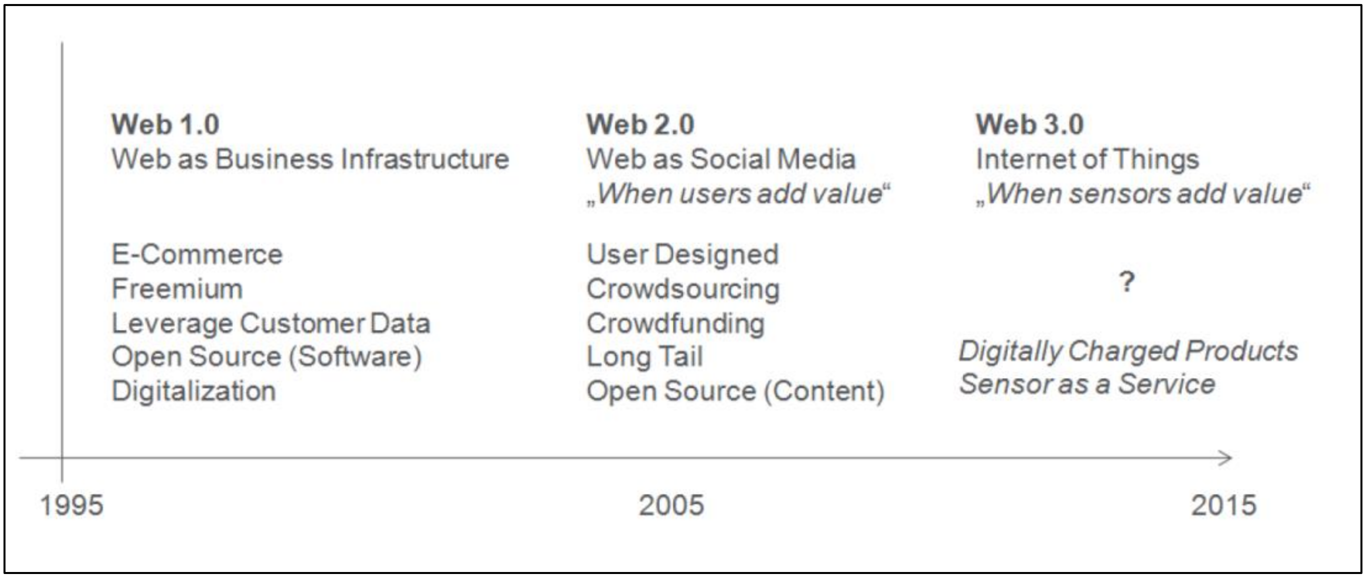


Figure 6: Internet wave and business model pattern timeline[88]

Each new internet wave has led to new digital ‘business model patterns’[89].

In Web 1.0 (see Figure 6 above), functions of traditional advertising and direct sales channels were complemented – if not completely overtaken – by the e-commerce business model pattern; 10 years later, internet platforms created “Social Media” that pulled in, facilitated, and matched interactions between participants, affording new concepts such as Crowdsourcing (Facebook, Craig’s List, Airbnb) and Crowdfunding (Kickstarter, Indiegogo), et al.[90] Just like in internet waves 1 and 2, never-before-known

[88] Source of Figure: Elgar Fleisch, Markus Weinberger and Felix Wortmann, “Geschäftsmodelle im Internet der Dinge,” [Business Models in the Internet of Things], December 2015, p. 454, available (in German) here: http://cocoa.ethz.ch/downloads/2016/09/2175_ZfbF_BM_IoT.pdf

[89] Gassman, et al, define “business model pattern” as a definite configuration of four core elements proven successful in different industries; the elements are (1) Who are the customers? (2) What is being sold? (3) How is it produced? and (4) How is revenue earned? See Oliver Gassmann,, Karolin Frankenberger, and MichaelaCsik “The St. Gallen Business Model Navigator” https://www.thegeniusworks.com/wp-content/uploads/2017/06/St-Gallen-Business-Model-Innovation-Paper.pdf, p. 2.

[90] G. Parker, M. Van Alstyne, S. Choudary, “Platform Revolution: How Networked Markets Are Transforming the Economy - and How to Make Them Work for You,” (New York, NY: W. W. Norton, 2016).; p.14

business models are being established today with IoT. Leveraging more than just connected people, Web 3.0—IoT already generates a new lever of value to cities, communities and their related enterprises;[91] the question this section attempts to address is

> '*What are the business models that are likely to enjoy the greatest degree of use and monetization success for Smart Cities and Connected Communities?'*

To determine whether there is a value for municipalities in investing in IoT technologies, the section offers a conceptual screen, i.e., the "EPIC Analysis" for IoT (section 4.3).

Before exploring the EPIC concept in detail, it is important to understand some key new IoT business models brought about by IoT. One approach, among many[92], is outlined below in three general categories:

- Digitally Charged Products
- Sensor as a Service/Data as a Service
- Platform Marketplaces

4.2 New Business Models

4.2.1 Business Model Logic

Back in 2014, researchers at the Bosch Internet of Things and Services Lab and the University of St. Gallen in Switzerland analyzed 55 business model patterns from a research paper from Oliver Gassmann et al.[93] and many Internet of Things applications with regard to their value - creating steps and high-resolution management. They derived a very general business model logic for the Internet of Things and some specific components and patterns for business model, which still today provide a solid and useful guide for action.

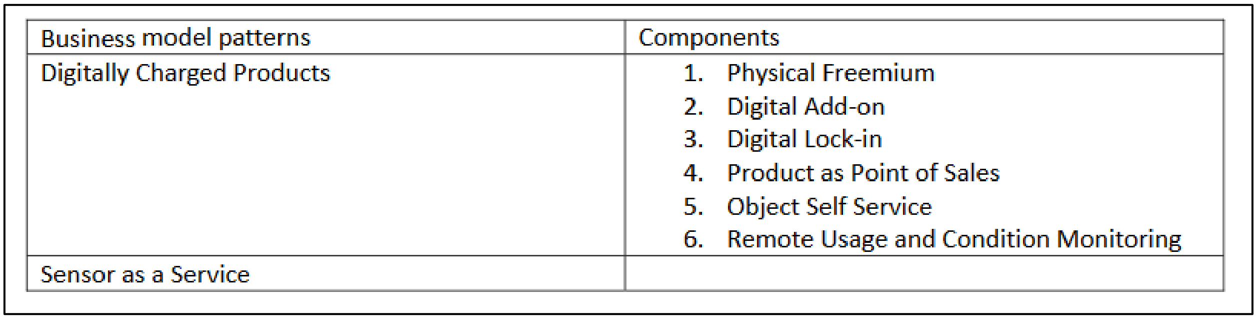
> *"The results of this analysis can be represented as six components for business model patterns and two independent business model patterns for the Internet of Things. Based on their power and their kinship – all of them facilitate digital services for physical products – we merge them all together in a new business model pattern specific to the Internet of Things, Digitally Charged Products. On the*

[91] McKinsey Global Institute, The Internet of Things: Mapping the Value Beyond the Hype, June 2015, executive summary and full report can be found here: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[92] See for example this recent article on how monetization of consumer IoT capabilities can help drive new business models: Gloria Rismondo, "The Monetization of IoT Solutions," Global Payments Blog Website, December 20, 2017, https://www.globalpaymentsinc.com/en-us/blog/2017/12/20/the-monetization-of-iot-solutions

[93] Gassmann, Oliver; Frankenberger, Karolin; Csik, Michaela:"The Business Model Navigator: 55 Models That Will Revolutionise Your Business," Harlow: Pearson, 2014, See also "The St. Gallen Business Model Navigator" op. cit.

> *other hand, the concept of Sensor as a Service is so novel and so powerful that we suggest that it is itself a new business model pattern (see Table 2).”*[94]



Business model patterns	Components
Digitally Charged Products	1. Physical Freemium 2. Digital Add-on 3. Digital Lock-in 4. Product as Point of Sales 5. Object Self Service 6. Remote Usage and Condition Monitoring
Sensor as a Service	

Table 2: Components and Business Model Patterns in the Internet of Things

4.2.2 Digitally Charged Products

Physical Freemium is a physical asset that is sold together with a free digital service, which is "attached" to the product at no additional charge. Over time, a percentage of customers will select premium services that go beyond the free ones and are then invoiced. Examples for homes**:** Nest (familiar face alerts, live video streaming)**,** Ring (recorded video storage of persons approaching the home)**.**

Digital Add-on is a monetization method whereby a physical asset is sold very inexpensively and therefore at a small margin. Over time, the customer can purchase or activate any number of digital services with a higher margin. For example, when an automobile’s performance can be configured using software and the vehicle is a node on the internet, then the customer can purchase an additional 50 horsepower for an upcoming weekend.

Digital Lock-in is analogous to the Razor and Blade business model in the physical world: It is a sensor-based, digital handshake that is deployed to limit compatibility, prevent counterfeits, and ensure warranties. For cities, digital lock-in could be combined with the Sensor as a Service model (below) to prevent sensor data—licensed by cities to proprietary app developers—from being copied, transferred or otherwise resold or used insecurely outside a city’s digital marketplace.

*Product as Point of Sales***:** Physical items or commercial products become sites of digital sales and marketing services that the customer consumes directly at the product or indirectly via a smart phone. Any object can carry digital advertising, and the product itself collects and transmits loyalty points and records the world around it. Examples include

[94] Elgar Fleisch (ETH Zurich / University of St. Gallen), Markus Weinberger (Bosch Software Innovations GmbH), Felix Wortmann (University of St. Gallen), “Business Models and the Internet of Things”, August 2014, Bosch IoT Lab http://www.iot-lab.ch/wp-content/uploads/2014/11/EN_Bosch-Lab-White-Paper-GM-im-IOT-1_3.pdf

smart billboards that allow cities to monetize city assets through digital ads, and consumers that can place orders/re-orders, etc.

Thing (or Object) Self Service: “Things” can independently place orders via a web-service call (modeling a replenishment order) to a utility. For example, a building heating system could order oil refills as soon as a certain level of liquid is noted in the oil tank. The idea of self-service no longer refers only to the customer; now things can serve themselves too.

Remote Usage and Condition Monitoring: "Smart" things can transmit data about their own status or their environment in real time. This makes it is possible to detect out-of-tolerance conditions preventatively, monitor usage and the remaining inventory of consumables, or to monitor the environment (temperature, light, traffic, etc.) around the sensor. Some notable examples include: Ride usage, mileage, air pressure of shared city bicycles, and city infrastructure monitoring.

4.2.3 Sensor as a Service/Data as a Service

Data-generating products and services are not the focus but rather the data itself: collecting, processing, and selling sensor data for a fee. For example, a manufacturer of IoT light fixtures affixes sensors that track everything from how much power the lights consume to traffic under the post, ambient light, and temperature. More sophisticated sensors can measure pollution levels, radiation, traffic, etc. Data collected is shared with the owner of the land and sold to third party developers; revenue is split between the manufacturer and the owner of the land.[95] As for smart parking, municipalities have not only installed sensors on lampposts but beneath parking spaces to detect vacant parking places. Data generated from sensors is sold to third parties for mobile app development for consumer use. City governments benefit since the real-time nature of the data identifies parking offenders without the traditional labor and time-intensive activities; moreover, utilization of parking places increases, and therefore so does revenue, since parking tenants can set up automatic payments to expired meters.

4.2.4 Platform Marketplaces

Unlike traditional Pipeline Business Models—whereby suppliers upstream feed producers who use their resources to manufacture and sell to consumers at the other end of the supply chain—platform businesses like the Apple App Store and Airbnb connect producers, consumers, and some who play both roles to exchange or co-create something of value for all participants.

With platforms, the internet no longer acts like a distribution channel (a pipeline) but rather a creation infrastructure—platforms create value, using resources they do not own.

[95] Leo Merani, “These companies are mining the world’s data by selling street lights and farm drones,” Quartz, March 25, 2014 https://qz.com/191545/these-companies-are-mining-the-worlds-data-by-selling-street-lights-and-farm-drones/

Platforms afford network effects (more production leading to more consumption and vice-versa) so that platforms grow faster and at minimal marginal costs. Platforms can embrace millions of remote participants, thereby offering a value creation capacity larger than that of the value created by a traditional municipality.[96]

As an example, Chicago's digital hub platform sponsors hackathons and other activities to "serve as an innovative tool to improve the lives of all residents".[97] Likewise, Santander, Spain's open data portal encourages start-ups to create a wide range of apps for its citizens. [98] Los Angeles' data platform claims to have helped open 34,000 new businesses.[99]

In the IoT space, platforms are as equally important; they aim to simplify and optimize operations as summarized in this 2017 *McKinsey* article on IoT platforms:

> *"In the Internet of Things, platforms are designed to deploy applications that monitor, manage, and control connected devices. IoT platforms must handle problems like connecting and extracting data from a potentially vast number and variety of endpoints, which are sometimes in inconvenient locations with spotty connectivity"*[100]

As of June 2017, the Hamburg, Germany-based research firm *IoT Analytics* observed that the IoT platform market remains fragmented with 450+ vendors[101]. Why such a big number of IoT platform vendors? The above-mentioned *McKinsey* piece advances the following explanation:

> *"Why so many platforms? Look at successful software platforms like Windows for operating systems. Platforms make a lot of money and are high-margin franchises that endure for decades. People and companies don't switch platforms very often. Often, switching costs are significant and platform choices persist for many years."*[102]

According to *IoT Analytics*, the IoT platform market will reach over US$ 22 billion by 2023 – see Figure 7 below (five platform types are included: cloud platforms, application enablement platforms, device management platforms, connectivity platforms, advanced analytics platforms)

[96] See G. Parker, M. Van Alstyne, S. Choudary, "Platform Revolution etc.", op. cit.

[97] "How Chicago Is Growing Its Open Data Economy," https://socrata.com/case-study/chicago-growing-open-data-economy/ .

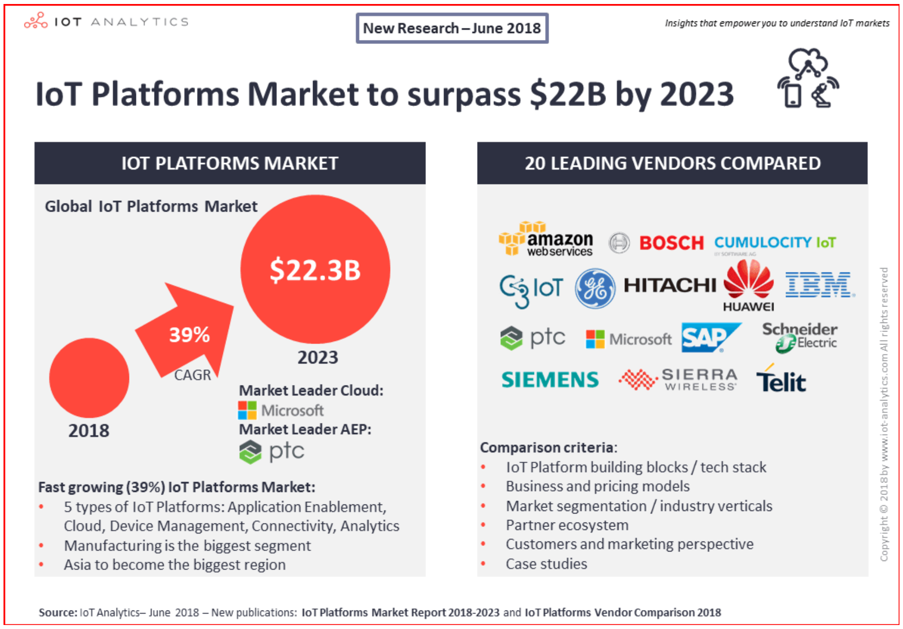
[98] https://www.europeandataportal.eu/en/news/four-new-applications-developed-open-data-city-santander

[99] http://www.govtech.com/dc/digital-cities/Digital-Cities-Survey-2016-Winners-Announced.html

[100] Eric Lamarre and Brett May, "Making Sense of Internet of Things Platforms," May 2017, McKinsey, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/making-sense-of-internet-of-things-platforms

[101] Source: IoT Analytics, "IoT Platform Comparison: How the 450 providers stack up," July 13, 2017 https://iot-analytics.com/iot-platform-comparison-how-providers-stack-up/

[102] Lamarre and May, op. cit.



IoT Platforms Market to surpass $22B by 2023

IOT PLATFORMS MARKET

Market Leader Cloud: Microsoft

Market Leader AEP: ptc

Fast growing (39%) IoT Platforms Market:

- 5 types of IoT Platforms: Application Enablement, Cloud, Device Management, Connectivity, Analytics
- Manufacturing is the biggest segment
- Asia to become the biggest region

20 LEADING VENDORS COMPARED

Comparison criteria:

- IoT Platform building blocks / tech stack
- Business and pricing models
- Market segmentation / industry verticals
- Partner ecosystem
- Customers and marketing perspective
- Case studies

Source: IoT Analytics– June 2018 – New publications: **IoT Platforms Market Report 2018-2023** and **IoT Platforms Vendor Comparison 2018**

Figure 7: IoT platforms market, US$ million 2018 -2023[103]

4.2.5 IoT Platform Challenges

While early IoT platform developers tried to create universal tools that could be applied across a wide variety of market verticals, many of them have come to realize that it was too ambitious an objective. Figure 8 below illustrates the multifaceted challenges that must be overcome:

4.2.5.1 The set of given parameters

Any IoT platform must be *trustworthy*, i.e., be secure, private, safe, reliable, and resilient (based on the Cyber-physical systems (CPS) framework recommendations from the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce[104]), and be able to bridge with the past (legacy integration[105]) and the future (future-proofing[106]) regardless of the location – in short, be operational *anytime and anywhere*.

[103] Source: IoT Analytics Press Release," Microsoft and PTC named leading IoT Platform vendors for Cloud and AEP, respectively, as growth in the IoT Platforms Market accelerates to 39%," June 26, 2018 https://iot-analytics.com/report-us22-billion-iot-platforms-market-by-2023/. Note that Berg Insight, which researched a narrower IoT platform market, i.e., connectivity management platforms, device management platforms and application enablement platforms, estimates (as of June 2018) that the IoT platform market will reach US$ 7.1 billion in 2022 http://www.berginsight.com/ReportPDF/ProductSheet/bi-platforms3-ps.pdf

[104] See Section 3.2 IoT Security.

[105] See Jason Kay, "Putting legacy systems at the heart of IoT," Internet of Things Agenda, May 25, 2017 https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Putting-legacy-systems-at-the-heart-of-IoT

[106] See Benson Chan, "How to Future-Proof Your IoT Infrastructure Investment," IoT for All, July 3, 2017. https://www.iotforall.com/how-future-proof-iot-infrastructure/ . Another innovative perspective on "future-

4.2.5.2 The variables

An effective universal platform must be able to accommodate any volume and data rate, i.e., not requiring “reinventing the wheel” as the needs expand (*scalabililty*). At the same time, it must be able to navigate through different communication protocols and allow the integration of various information networks, e.g., cellular, WiFi, and satellite in the case of tracking services (*interconnectability*). Finally, “what’s good for the goose should be good for the gander,” meaning that the platform should be capable, for example, of handling healthcare as well as energy or automotive IoT solutions (*extensibility*).

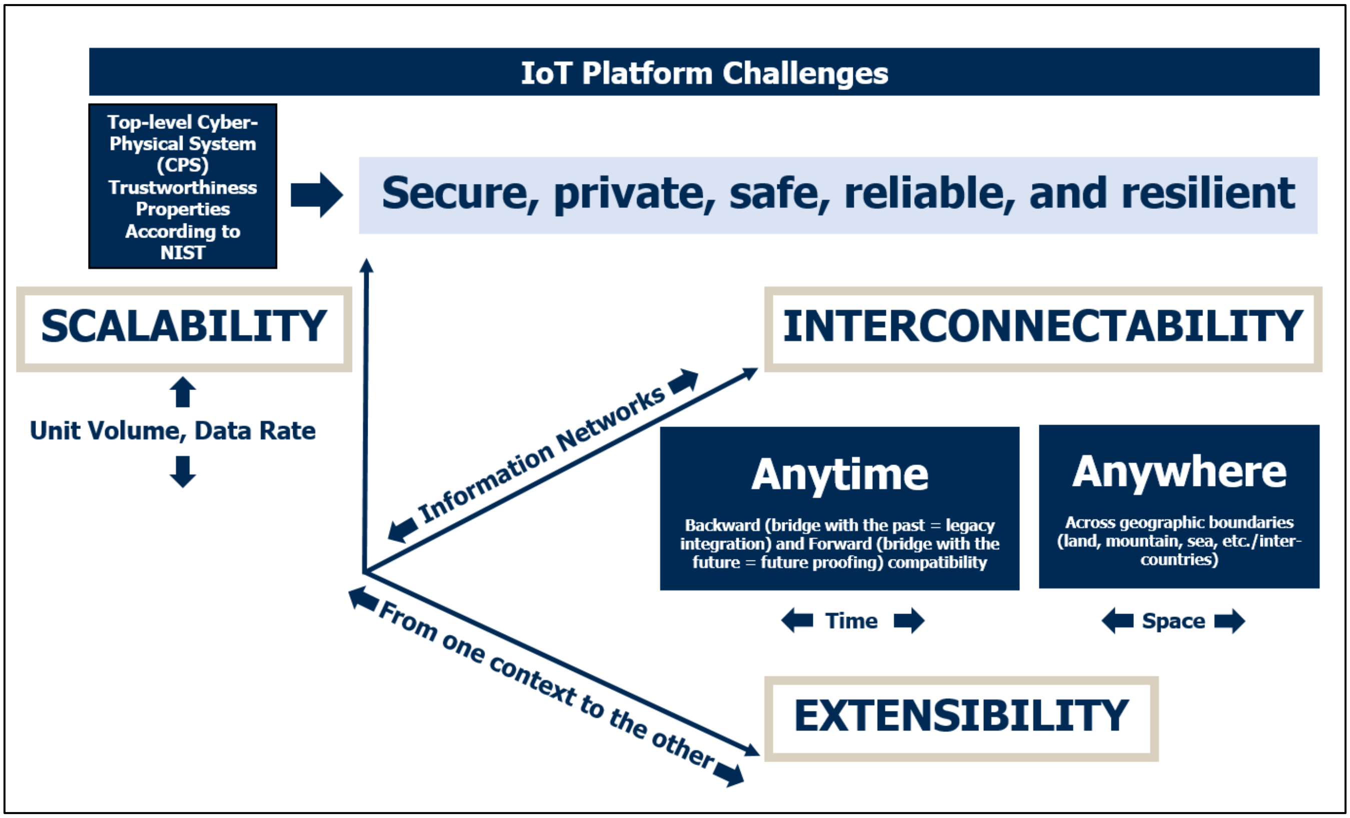

IoT Platform Challenges
Top-level Cyber-Physical System (CPS) Trustworthiness Properties According to NIST
Secure, private, safe, reliable, and resilient
SCALABILITY
Unit Volume, Data Rate
INTERCONNECTABILITY
Information Networks
Anytime
Backward (bridge with the past = legacy integration) and Forward (bridge with the future = future proofing) compatibility
Anywhere
Across geographic boundaries (land, mountain, sea, etc./inter-countries)
Time
Space
From one context to the other
EXTENSIBILITY

Figure 8: IoT Platform Challenges[107]

Note: *The trustworthiness properties in Figure 8 are limited to those applied most broadly across the whole spectrum of IoT applications as observed by NIST. However, additional trustworthiness dimensions can certainly be added based on system functionality and operational needs.*

proofing” can be found in Prof. Jonathan Zittran’s article on “From Westworld to Best World for the Internet of Things,’ *The New York Times*, June 3, 2018, https://www.nytimes.com/2018/06/03/opinion/westworld-internet-of-things.html where the author proposes “unusual solutions” (i.e., “networked safety bonds” and “work by nonprofit foundations to maintain the code for abandoned products”) to confront the “life-cycle problem”.

[107] Source: Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT)

Based on CDAIT's interaction with IoT stakeholders, time proofing (vs. past and future), and scalability appear to be the most pressing challenges. As far as legacy integration, the below observation provides a good summary of related hurdles standing in the way:

> *"Manufacturers who want to engage in this process already have a lot of legacy hardware, embedded software and firmly established production lines. These have been developed from years of experience and quality testing, and companies would rather stick to them when making design decisions and technical choices rather than spend huge amounts of money to move into new, uncharted territory. That's why many brands and enterprises remain wary about getting involved in IoT, despite acknowledging its potential impacts."*[108]

The strategic imperative of protecting against premature obsolescence[109], i.e., ensuring forward compatibility, is well captured in the following comment:

> *"What becomes clear is that truck rolls are an IoT investment killer. In each case, the device life needs to be at least as long as the expected years in service in order to be profitable. As soon as a truck roll is required, the expected savings disappear. In order for an IoT investment to make sense, the savings have to increase 28-fold even to be considered."*[110]

The arrival of eSIM (embedded Subscriber Identity Module) a.k.a., eUICC (embedded Universal Integrated Circuit Card), a GSMA global specification enabling remote SIM provisioning of any mobile device, is a critical milestone toward future proofing in the IoT arena. Regarding scale, IoT solution providers in search of the elusive universal platform are, for the time being, coming back empty-handed:

> *"Because of often minor (and sometimes major) differences between locations, environments, equipment, personnel, processes and many other factors, the solutions put together in one context often do not work in another. Early adopters of Internet of Things products and technologies in business environments have started to discover that these scale challenges are very real. As a result, their IoT deployments are moving at a much slower pace than they originally hoped/…/ The need for highly specialized and highly customized solutions makes IoT difficult to scale/…/IoT in business environments is not a product or even a technology, it's a process. That makes it extremely challenging to scale."* [111]

[108] Joe Britt, "Here's your first tech buzzword of 2017: 'Brownfield'," Recode, December 14, 2016 https://www.recode.net/2016/12/14/13925096/iot-brownfield-development-internet-of-things-greenfield-afero

[109] A telling example is provided by Frederic Paul in "IoT has an obsolescence problem," Network World, June 11, 2018 https://www.networkworld.com/article/3279729/internet-of-things/iot-has-an-obsolescence-problem.html#tk.rss_internetofthings

[110] Ingenu website, "Without Device Longevity, the Internet of Things Will Never Be", January 19, 2016, https://medium.com/achieving-the-grand-vision-of-the-internet-of/without-device-longevity-the-internet-of-things-will-never-be-58c904703abb

[111] Bob O'Donnell, "The Internet of Things is facing challenges with scale," Recode, June 22, 2016 https://www.recode.net/2016/6/22/11991414/internet-of-things-iot-challenges-scale

4.2.6 Side Note on Artificial Intelligence

The amount of data generated daily by observations of IoT assets is staggering. Traffic management for a single asset in a major city could easily surpass a million observations in a single day. Without Artificial Intelligence (AI), extracting value from the large amounts of data will be extremely difficult. AI will be the cement that will hold the complexities of Smart City data together to produce services of value. IoT business models will likely incorporate AI to drive their functional value propositions. Callum McLelland, managing editor of *IoT for All*, offers a vivid picture of the tight relationship between AI and IoT:

> ***"AI and IoT are Inextricably Intertwined*** *- I think of the relationship between AI and IoT much like the relationship between the human brain and body. Our bodies collect sensory input such as sight, sound, and touch. Our brains take that data and makes sense of it, turning light into recognizable objects and turning sounds into understandable speech. Our brains then make decisions, sending signals back out to the body to command movements like picking up an object or speaking. All of the connected sensors that make up the Internet of Things are like our bodies, they provide the raw data of what's going on in the world. Artificial intelligence is like our brain, making sense of that data and deciding what actions to perform. And the connected devices of IoT are again like our bodies, carrying out physical actions or communicating to others."*[112]

However, regardless of the outstanding AI achievements, close-at-hand or soon within reach, we need to remain cautious about how the utilization of AI will unfold.

When a European Parliament resolution introduced the possibility of granting special legal status, or "electronic personalities," to sophisticated robots, specifically those that can make autonomous decisions or otherwise interact with third parties independently, it was met with resolute resistance from 156 robotics, legal, medical, and ethics experts who brought the expectations down to reality in an open letter in April 2018:

> *"From a technical perspective, this statement [i.e., February 16, 2017, European Parliament Resolution on Civil Law Rules of Robotics] offers many bias based on an overvaluation of the actual capabilities of even the most advanced robots, a superficial understanding of unpredictability and self-learning capacities and, a robot perception distorted by Science-Fiction and a few recent sensational press announcements."*[113]

[112] Calum McClelland, "The Difference Between Artificial Intelligence, Machine Learning, and Deep Learning," IoT for All, February 23, 2017, https://www.iotforall.com/the-difference-between-artificial-intelligence-machine-learning-and-deep-learning/

[113] Open Letter to the European Commission Artificial Intelligence and Robotics, released on April 12, 2018, https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf. The letter quotes the February resolution which

In a June 2018 essay for *The Atlantic*, Dr. Henry Kissinger, describing the potentials and perils of AI, warns about the uncertainly surrounding its results:

> *"Artificial intelligence will in time bring extraordinary benefits to medical science, clean-energy provision, environmental issues, and many other areas. But precisely because AI makes judgments regarding an evolving, as-yet-undetermined future, uncertainty and ambiguity are inherent in its results."*[114]

4.3 THE EPIC ANALYSIS FOR IOT

The "EPIC" analysis for IoT is a concept that can help municipalities (and any other organized collectivity in charge of the public interest, which is exploring the potential use of IoT technologies) review the opportunity and impact of investing in IoT. EPIC[115] screens the IoT effort through four variables: *Ethics, Profit (economic and social), Intimacy,* and *Connectivity*[116].

4.3.1 Ethics

- Ethical implementation of intelligent (including IoT-related) technologies is receiving a lot of focused attention worldwide as demonstrated by the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems[117]:

recommended "Creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently."

[114] Henry Kissinger, "How the Enlightenment Ends Philosophically, intellectually—in every way—human society is unprepared for the rise of artificial intelligence," The Atlantic, June 2018 issue, https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/

[115] Adapted and expanded from the 4Cs concept (Closeness, Convenience, Connectivity and Cash) developed by Johnny Parham. Note that it is also different from another 4Cs IoT model proposed by Kumar Srivastava at IDG (Categorization, Calibration, Control and Collection: https://www.cio.com/article/2908902/cio-role/4-fundamental-cs-of-iot-architecture-and-design.html) or the one identified by IHS Markit (Connect, Collect, Compute and Create: http://news.ihsmarkit.com/press-release/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says). Back in 2013, Lopez Research in a White Paper on "An Introduction to the Internet of Things" proposed the "3Cs of IoT" (Communication, Control and Automation, and Cost Savings: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf)

[116] It must be noted that the EPIC acronym is not related to the EPIC (Electronic Privacy Information Center) organization, which, however, must be recognized for its work on privacy issues related to the Internet of Things, see: https://epic.org/privacy/internet/iot/

[117] See for example: IEEE Press Release on "IEEE Global Initiative for Ethical Considerations in Artificial Intelligence (AI) and Autonomous Systems (AS) Drives, Together with IEEE Societies, New Standards Projects; Releases New Report on Prioritizing Human Well-Being,", July 19, 2017 https://www.businesswire.com/news/home/20170719005136/en/IEEE-Global-Initiative-Ethical-Considerations-Artificial-Intelligence

> *"To be able to contribute in a positive, non-dogmatic way, we, the techno-scientific communities, need to enhance our self-reflection, we need to have an open and honest debate around our imaginary, our sets of explicit or implicit values, our institutions, symbols and representations.*
>
> *Eudaimonia, as elucidated by Aristotle, is a practice that defines human well-being as the highest virtue for a society. Translated roughly as "flourishing," the benefits of eudaimonia begin by conscious contemplation, where ethical considerations help us define how we wish to live.*
>
> *Whether our ethical practices are Western (Aristotelian, Kantian), Eastern (Shinto, Confucian), African (Ubuntu), or from a different tradition, by creating autonomous and intelligent systems that explicitly honor inalienable human rights and the beneficial values of their users, we can prioritize the increase of human well-being as our metric for progress in the algorithmic age. Measuring and honoring the potential of holistic economic prosperity should become more important than pursuing one-dimensional goals like productivity increase or GDP growth."*[118]

- When developing and deploying any IoT solution, one must always remember the adage, "Just because I can, doesn't mean I should." Before (from the outset, by design) and during the implementation of any IoT device/service, ethical considerations must remain front and center to ensure that, as it changes, the system serves its purpose without undesirable impacts, be they on individuals, groups, the environment, the economy, or society as a whole.

- A recent article[119] on the ethical responsibilities of design engineers of self-driving cars (a prototypical example of applied IoT technologies) by Jason Borenstein, Joseph Herkert, and Keith Miller (Borenstein et al.) provides a helpful review of a diverse range of perspectives on the topic and underlines a set of "rules" championed by Keith Miller in collaboration with other computer scientists, engineers, and ethicists, which were created with the intent of providing guidance to the computing and engineering communities especially with respect to pervasive and autonomous technologies [120]. The following unequivocal "Rule 1" is highlighted in the paper:

  > *"The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is*

[118] IEEE, "Ethically Aligned Design - A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems," Version 2 for public discussion released on December 12, 2017 [final version to be released in 2019], p. 2 https://standards.ieee.org/develop/indconn/ec/ead_v2.pdf

[119] Jason Borenstein, Joseph R. Herkert, Keith Miller, "Self-Driving Cars: Ethical Responsibilities of Design Engineers," IEEE Technology and Society Magazine, June 1, 2017 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7947308&tag=1. Note: Dr. Jason Borenstein is the director of Graduate Research Ethics Programs and associate director of the Center for Ethics and Technology at Georgia Tech.

[120] Keith Miller, "Moral responsibility for computing artifacts: 'The Rules'," IT Professional, IEEE Computer Society pp. 57-59, May/June 2011; http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5779006

> *shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system."*[121]

Borenstein et al. offer this rule of thumb regarding ethical obligations:

> *"At an individual level, each designer should consider his/her ethical obligations in terms of creating safer technology. One approach that incorporates this type of thinking is value-sensitive design, which encourages designers to consider how the user's cherished values, such as autonomy, can be upheld while in the process of creating their technologies."*[122]

- Unethical behaviors, features, etc. of an IoT product/service will negate other values it may generate. A few examples of terms associated with ethical values, presented here as a non-authoritative guide only (food for thought), are accuracy, autonomy, choice, confidentiality, equity (impartiality, justice and fairness), freedom, honesty, inclusiveness, loyalty, respect, sincerity, timeliness, tolerance and truth.
- In the EPIC model, ethical considerations are the set of "explicit or implicit values" that "prioritize the increase of well-being", which must be satisfied for the successful deployment of IoT services.
- Table 3 below, which was assembled by researchers in Europe, i.e., Gianmarco Baldini, Maarten Botterman, Ricardo Neisse and Mariachiara Tallacchini, in a June 2018 paper on Ethical Design in the Internet of Things, outlines the related challenges, and may provide some guidance to IoT developers in determining "ethical musts".

[121] Borenstein et al. op. cit.
[122] Borenstein et al., op. cit.

#	Challenge	Description
1	Economic incentives for data protection of the user are not directed to the user	Economic incentives for data protection of the user are limited to the businesses creating the IoT applications and devices
2	Incomplete information on the consequence of data disclosure	The user has often incomplete information about the consequences of disclosing data either voluntarily (e.g., providing data) or involuntarily (e.g., collection of position information). This lack of information affects each privacy decision. The incomplete information can also be a consequence of a limited perception by the user (e.g., the digital divide problem). In the IoT, this issue could be more relevant than in the Internet as the physical world information (e.g., physical position) could increase the information space. This is related to a concept of *transparency* on how disclosed data is used by the developer of the IoT system or application
3	Too large information space about the consequence of data disclosure	The complete set of needed information to make a rational choice could be so large that the user may not be able to access the IoT service in an effective way
4	Psychological biases	For example, the perception of immediate benefits (e.g., free access to an IoT service or application) can impact the long-term negative impact (e.g., risk to users' privacy)
5	Trade-offs between businesses needs to collect and process data and rights to privacy	There is something of a tension between the market's needs for data collection and correlation to support innovation and the business success of the IoT systems and applications (for both the public and private sector) and the protection of users' data. While government (e.g., regulators' bodies) may support the balance on one or another direction, one significant challenge is to design and apply regulations in a very dynamic environment where the life-cycle of the IoT applications in the market can be much shorter than the regulatory process
6	Cost of implementing privacy enhancing or data protection solutions	The costs of implementing PET (Privacy Enhancing Technologies), or other solutions to ensure proper care in collection, storage and retrieval of data. Who is going to support these costs? For example: that the willingness of the user to pay for the service, or the political will to ensure societal guarantees enforced through legislation
7	Accountability	The accountability of the IoT applications regarding users' privacy. Who is going to be legally accountable for the user's data? As seen in recent events, a data breach can be extremely damaging to a business company from an economic point of view. Are PET producers responsible for privacy breaches or the application where the PET is applied? Or the users themselves?
8	On-line and off-line identity	It is difficult to separate the on-line information from the off-line information and their linkage can generate privacy breaches
9	Digital divide	Users have different set of capabilities in accessing the IoT devices and applications. Depending on their level of technical proficiency, users have different levels of perceptions of the privacy risks or different understanding of the requests sent to them through the IoT
10	Conformance to regulatory frameworks	The definition, implementation and conformance to regulations in this context can be hampered by two factors: (1) the speed of the evolution of the IoT can be faster than the regulatory process itself, so that regulations can be moderately effective when they are enforced, (2) already deployed IoT systems and devices may require significant rework or replacement (e.g., recall of the IoT devices) which can be very expensive for companies
11	Support for dynamic context	The use of the IoT services and devices and the processing and storage of personal data may change depending on the context as recommended in Nissenbaum[123]

Table 3: Challenges for Ethical Design in IoT[124]

[123] Nissenbaum, H. (2015), "Respecting context to protect privacy: Why meaning matters. Science and Engineering Ethics," 2015, 1–22. (online preview) http://link.springer.com/article/10.1007%2Fs11948-015-9674-9

[124] Source: Quoted as-is from Gianmarco Baldini, Maarten Botterman, Ricardo Neisse and Mariachiara Tallacchini, "Ethical Design in the Internet of Things," Sci Eng Ethics (2018) 24: 905. https://doi.org/10.1007/s11948-016-9754-5

4.3.2 Profit

Profit here refers to both economic and social benefits.

- The notion of "economic profit" is straightforward. It is the positive financial return that all city stakeholders (private and public) receive from providing and/or using IoT devices/services. Since cities generally are non-profit entities whose financial objective is to minimize costs (under constraints such as fulfilling electoral promises), their economic benefit is the difference between costs before and after IoT; in other words, it boils down to productivity gains achieved with IoT technologies.
- On the other hand, "social profit" refers to the good done in and to the community (including protecting the environment and other elements related to the quality of life), and may or may not lead to an immediate monetary gain. Although sometimes difficult to quantify, social profit, a critical objective, must be integrated in the analysis:

  > *"But what we need is more social profit, from better schools to access to medical care, great art and music, clean rivers, high-functioning public transportation, and empowering young people to take care of themselves — anything that benefits people and their places and the planet we live on. 'But isn't social profit hard to measure?' you might ask. 'Yes!' I would exclaim. 'That's why I am writing about assessment. We have to find an approach to defining social profit that gives us the incentives, the motivation, and the confidence to invest in it.' /…/ Social profit is about desired social benefits, and so it has to be defined locally depending on what a community of people values and what they need. It will never have a fixed or standard measure, and efforts to create one will get bogged down in endless quibbles and conflict about the measure itself."*[125]

- Economic and social benefits can be tangible or intangible, direct or indirect (e.g., positive externalities[126]), but eventually serve the whole community.
- The Pierce and Andersson study quoted elsewhere in this White Paper, which explores the predominant challenges in Smart City initiatives from the municipal decision-

[125] David Grant, "The social profit handbook: Setting and achieving mission-driven goals," GreenBiz, August 8, 2015, https://www.greenbiz.com/article/social-profit-handbook-setting-and-achieving-mission-driven-goals. Note that the social dimension is an increasingly important topic of the current Smart City conversation, see for example, Dr. Kendra L Smith's article on "The Inconvenient Truth about Smart Cities," Scientific American, November 17, 2017, which contains a useful reference to the New Delhi-based Housing and Land Rights Network report on "India's Smart Cities Mission: Smart for Whom? Cities for Whom?" (embedded in the article) https://blogs.scientificamerican.com/observations/the-inconvenient-truth-about-smart-cities/ and also Jeremy Cowan, "Smart to Future Cities: Defining the Perfect Solution," IoT Institute, April 27, 2018 http://www.ioti.com/smart-cities/smart-future-cities-defining-perfect-solution

[126] "A positive externality exists if the production and consumption of a good or service benefits a third party not directly involved in the market transaction," Encyclopaedia Britannica https://www.britannica.com/topic/private-good#ref1189686

makers' perspectives in mid-sized[127] European cities, adds a sense of urgency for the generation of economic and social gains for Smart Cities:

> *"The interviews showed that the lack of validated business models as well as the challenges to show specific gains – economic as well as social – on smart city investments means that many cities will have a hard timer (sic) to come up with reliable arguments in order to secure financing for their smart city initiatives."*[128]

It follows that Smart City planners must consider both sides of the profit equation before investing in IoT and determine whether the related technologies will yield the whole gamut of desired economic and social benefits[129].

4.3.3 Intimacy

In this context, intimacy entails:

- *Ease of access*, i.e., is the IoT device/service user friendly, convenient?
- *Mutual openness*, i.e., do the IoT solutions facilitate the mutual and willing sharing of information between provider and user?[130]
- *Customized experience,* i.e., does the service take into account the user's particular conditions and needs (as opposed to a one-size-fits-all approach)?

Citizen/customer/user intimacy is not only about the city having a high-quality relationship with the various constituencies it serves (*ease of access* and *mutual openness*).

It is also about how the city is able to leverage the knowledge acquired through this relationship in order to shape its various services (*customized experience*) and achieve buy-in and optimal participation (adapted from a paper by François Habryn, Benjamin Blau,

[127] Cities are increasing in both size and number, e.g. in 2016, 1.7 billion people - 23 per cent of the world's population lived in a city with at least 1 million inhabitants, while by 2030, a projected 27 per cent of people worldwide will be concentrated in cities with at least 1 million inhabitants." However, mid-sized (under 500,000 inhabitants) cities will keep a substantial share of the urban population, i.e., 49% in 2016 and 45% in 2030. Source: United Nations, "The World's Cities in 2016," http://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf

[128] Pierce and Andersson, op. cit. p. 2812.

[129] The use of IoT technologies for social good within a city is a current topic of research around the world, see Dr. Mara Balestrini's presentation during the session on *A City in Common: how citizens are leading a new wave of impactful social innovation* at the *Connected Technologies for Social Good* Conference on February 14-15, 2018, in Brussels Belgium on "Data Commons in the Making - Experiences on Developing a Citizen-centered IoT," https://capssi.eu/wp-content/uploads/Mara_Balestrini_Presentation.pdf

[130] See Hui Guan and Kumming Wang, "The dimensions of Customer Intimacy Relationship and Measurement Scale Development Based on Customers' Perspective," 2012 International Symposium on Information Technology in Medicine and Education, IEEE Xplore Digital Library https://ieeexplore.ieee.org/document/6291473/citations?part=1

Gerhard Satzger, and Bernhard Kölmel on measuring customer intimacy for B2B services, see Figure 9 below).

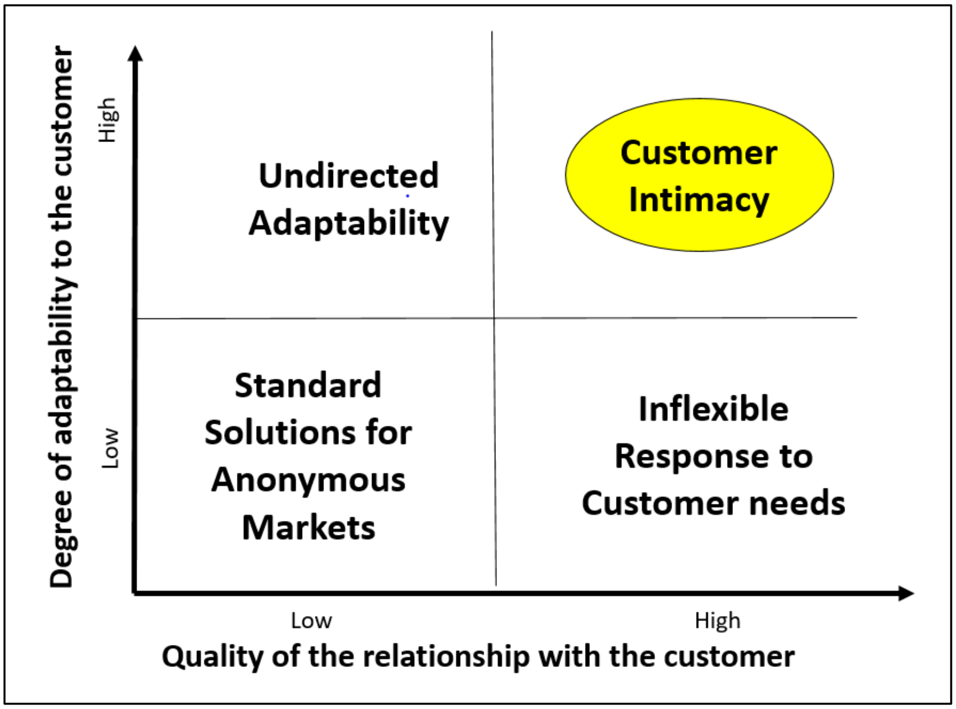

Degree of adaptability to the customer
High
Low
Undirected Adaptability
Customer Intimacy
Standard Solutions for Anonymous Markets
Inflexible Response to Customer needs
Low
High
Quality of the relationship with the customer

Figure 9: The Two Dimensions of Customer Intimacy[131]

Intimacy, as defined here, should be one of the key outcomes sought out by the ongoing digital transformation among Smart Cities as outlined below by Lai Weng Yew, Vice President of Business Application Services at NCS (SingTel, Singapore) in a 2016 interview on the digital transformation of the public sector:

> *"Digital Technologies", which NCS defines as Social, Mobility, Analytics, Cloud + Internet of Things (SMAC+I), enable the desired processes while "Digital Transformation" results in broader outcomes, which are customer intimacy, operational efficiency and digital business models. The implementation and adoption of "Digital Technologies" are part of the "Digital Transformation" journey."*[132]

How the contemplated IoT deployment fares on the (citizen/customer/user) intimacy scale is a critical question, which must be addressed up front.

[131] Source: Habryn, F., Blau, B., Satzger, G., & Kölmel, B. (2010), "Towards a Model for Measuring Customer Intimacy in B2B Services," Lecture Notes in Business Information Processing (pp. 1-14), Geneva, Switzerland: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14319-9_1
[132] Tan Wee Kwang, "Digital Transformation in the Public Sector," eGov Innovation, May 16, 2016 https://www.enterpriseinnovation.net/article/digital-transformation-public-sector-255850811

4.3.4 Connectivity

Connectivity is the overall technological foundation and includes:

- ***Medium***, i.e., how is the connection between parties made?[133]

  Most of the time, wireless connectivity will be the medium of choice. The following blurb ahead of the *Internet of Things (IoT) Summit* held in Anaheim, CA on January 14-15, 2018 at the *Radio Wireless Week 2018* sponsored by the Multi-Society IEEE Internet of Things Initiative (IoT) and the Microwave Theory and Techniques Society clearly lays out the reasons why wireless communications play a crucial role in IoT and the conditions for success:

  > *"While IoT is a very multi-disciplinary undertaking one of the indispensable elements is the exploitation and utilization of wireless technologies across a very broad set of applications for industry, the public sector, academia, and for individuals in their everyday life. For IoT to succeed the current connectivity and communication options face significant challenges. These include among others -- How to provide the bandwidth needs for IoT within the physical constraints of noise, propagation, building penetration, and safe energy budgets for wireless operation -- How to make efficient use of "good" spectrum that can accommodate the projected densities of IoT nodes without interference and with high availability -- How to deliver communications and connectivity to long lived sensors and actuators that have limited access to power sources -- How to live within the constraints of size and weight for many of the platforms that seek IoT connectivity -- How to provide the ubiquity needed for many of the IoT applications within the constraints of cost, performance, and sustainable business models."*[134]

  IoT devices are not all alike, and their need for connectivity varies widely; some (in great numbers) send a few bytes infrequently ("Massive IoT"), while others require always-on high-bandwidth connectivity with very low latency ("Critical IoT") – Figure 10 depicts the difference between Massive IoT and Critical IoT.

[133] A thorough and recent review of widely adopted IoT connectivity technologies and standards for IoT networking can be found in Anna Gerber, "Connecting all the things in the Internet of Things - A guide to selecting network technologies to solve your IoT networking challenges," IBM, January 3, 2018 https://www.ibm.com/developerworks/library/iot-lp101-connectivity-network-protocols/iot-lp101-connectivity-network-protocols-pdf.pdf - See also Daniel Alsen, Mark Patel, and Jason Shangkuan, "The future of connectivity: Enabling the Internet of Things," McKinsey & Company, November 2017 https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things

[134] IEEE Internet of Things, Internet of Things (IoT) Summit at RWW2018, http://sites.ieee.org/rww-2018/the-crucial-role-of-wireless-communications-in-iot/

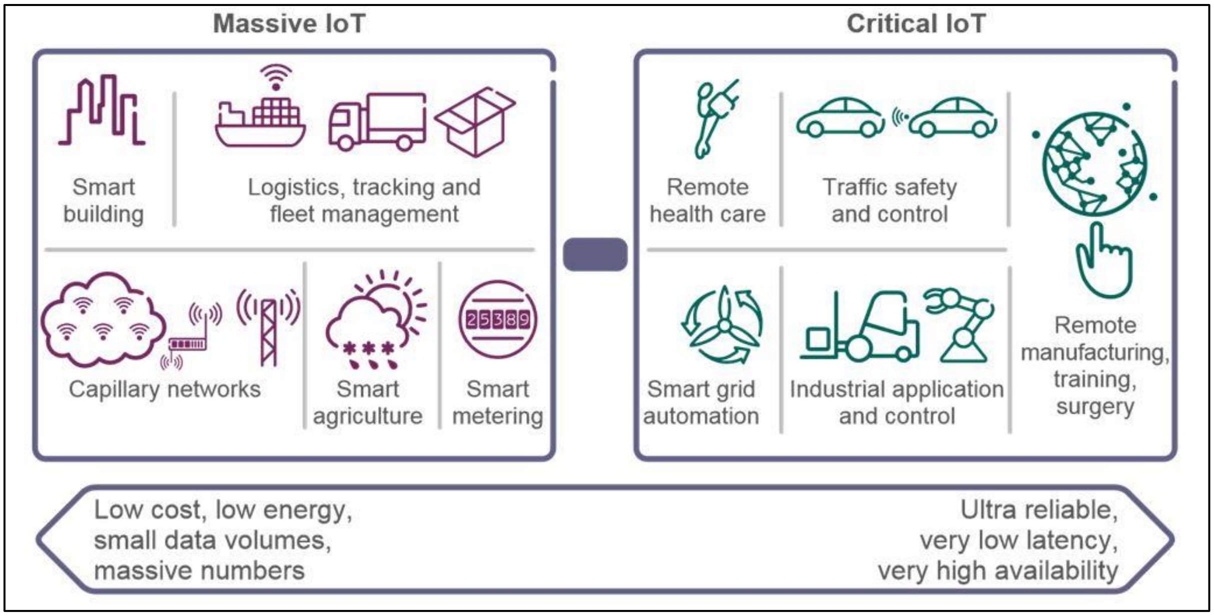

Massive IoT
Critical IoT
Smart building
Logistics, tracking and fleet management
Capillary networks
Smart agriculture
25389
Smart metering
Remote health care
Traffic safety and control
Smart grid automation
Industrial application and control
Remote manufacturing, training, surgery
Low cost, low energy, small data volumes, massive numbers
Ultra reliable, very low latency, very high availability

Figure 10: Massive IoT and Critical IoT[135]

- ***Computing,*** i.e., How and where is the transported data processed/analyzed?

  Where and to what degree the data captured by the physical interface (e.g., sensor) is going to be processed is a key and foundational element of any deployment of IoT technologies (see related discussion in above section 3.3.2 on utilities).

  Depending on several factors such as latency, availability, reliability and analytical needs, data processing should take place at the cloud, fog or edge levels (separately or in concert).

  The NIST definition, published in 2011, remains a good starting place for understanding the purpose of cloud computing (i.e., processing in a centralized data center, generally far away from end-users):

  > *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[136]

  In March 2018, NIST provided a useful distinction between fog computing and edge computing:

[135] Source: Vicki Livingston, "Putting the M and the C into 5G cellular IoT," IoT Agenda, November 2, 2017 https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Putting-the-M-and-the-C-into-5G-cellular-IoT

[136] Peter Mell and Timothy Grance, NIST Special Publication 800-145, "The NIST Definition of Cloud Computing," https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf . Note that NIST's cloud model is composed of five essential characteristics, three service models, and four deployment models.

> *"For the purpose of this document, the edge computing is the network layer encompassing the end-devices and their users, to provide, for example, local computing capability on a sensor, metering or some other devices that are network-accessible. This peripheral layer is also often referred to as IoT network. Fog computing is often erroneously confused with edge computing, but there are key differences* [137] *between the two concepts. Fog computing runs applications in a multi-layer architecture that decouples and meshes the hardware and software functions, allowing for dynamic reconfigurations for different applications while performing intelligent computing and transmission services. Edge computing runs specific applications in a fixed logic location and provides a direct transmission service. Fog computing is hierarchical, where edge computing tends to be limited to a small number of peripheral devices. Moreover, in addition to computation, and networking, fog computing also addresses storage, control and data - processing acceleration."*[138]

With more computing power available at a tiny scale (Moore's Law)[139], edge and fog computing, which have closer proximity to end-users and wider distribution than cloud computing, are becoming attractive options in IoT:

> *"With the development of IoT, edge computing is becoming an emerging solution to the difficult and complex challenges of managing millions of sensors/devices, and the corresponding resources that they require. Compared with the cloud computing paradigm, edge computing will migrate data computation and storage to the "edge'' of the network, nearby the end users. Thus, edge computing can reduce the traffic flows to diminish the bandwidth requirements in IoT. Furthermore, edge computing can reduce the transmission latency between the edge/cloudlet servers and the end users, resulting in shorter response time for the real-time IoT applications compared with the traditional cloud services. In addition, by reducing the transmission cost of the workload and migrating the computational and communication overhead from nodes with limited battery resources to nodes with significant power resources, the lifetime of nodes with limited battery can be extended, along with the lifetime of the entire IoT system."*[140]

[137] See OpenFog Consortium's whitepaper: https://www.nebbiolo.tech/wp-content/uploads/whitepaper-fog-vs-edge.pdf. IEEE announced on June 26, 2018 its adoption of the OpenFog Reference Architecture as official standard for fog computing https://www.openfogconsortium.org/news/ieee-adopts-openfog-reference-architecture-as-official-standard-for-fog-computing/

[138] Michaela Iorga, Larry Feldman, Robert Barton, Michael J . Martin, Nedim Goren, and Charif Mahmoudi, NIST Special Publication 500-325 on "Fog Computing Conceptual Model", March 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf

[139] See Alain Louchez, "The Internet of Things in Search of Critical Mass - How the growth of IoT is impacted by Moore's Law, Cooper's Law and Metcalfe's Law," Automation World, August 31, 2017 https://www.automationworld.com/article/internet-things-search-critical-mass

[140] Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, and Xinyu Yang "A Survey on the Edge Computing for the Internet of Things," IEEE Access, March 9, 2018 version, Digital Object Identifier 10.1109/ACCESS.2017.2778504, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8123913

Figure 11 (NIST) shows the interaction between the cloud, fog and edge[141] layers.

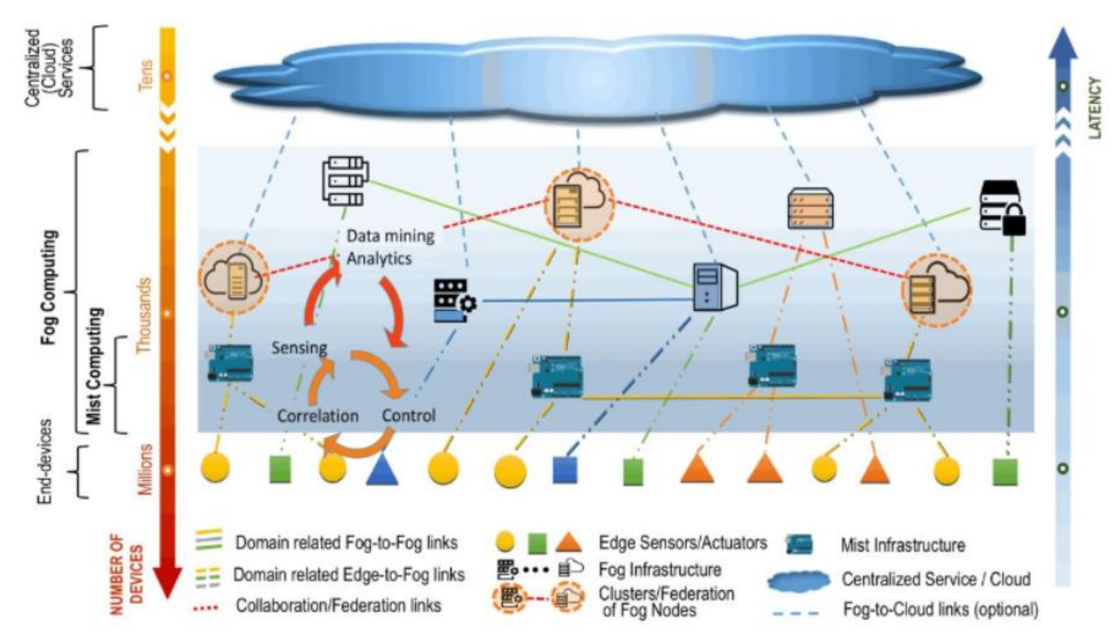

Centralized (Cloud) Services
Fog Computing
Mist Computing
End-devices
Tens
Thousands
Millions
NUMBER OF DEVICES
LATENCY
Data mining
Analytics
Sensing
Correlation
Control
Domain related Fog-to-Fog links
Domain related Edge-to-Fog links
Collaboration/Federation links
Edge Sensors/Actuators
Fog Infrastructure
Clusters/Federation of Fog Nodes
Mist Infrastructure
Centralized Service / Cloud
Fog-to-Cloud links (optional)

Figure 11: Fog computing support of a cloud-based ecosystem for smart devices)[142]

- ***Trustworthiness,*** i.e.**,** how much can the whole connectivity system (the "technological conduit") be trusted?

  Trust in the overall quality of connectivity (in the broad sense given here) requires several criteria to be satisfied. As mentioned elsewhere in this report, while security, privacy, safety, reliability and resilience are foremost trust-enabling properties, other dimensions could be added.[143]

  In a recent article on trusting Smart Cities for *Small Wars Journal*, Margaret L. Loper, CDAIT's Chief Technology Officer, discusses how trust applies to Smart Cities as well as the imperative need to be prepared:

  > *"In the coming decades, we will live in a world surrounded by tens of billions of devices that will interoperate and collaborate to deliver personalized and autonomic services. This paradigm of objects and things ubiquitously surrounding us is called the Internet of Things (IoT). Cities may be the first to benefit from the IoT, but reliance on these machines to make decisions has profound implications for trust. Trusting smart cities refers to the confidence and belief of smart city installations to be capable*

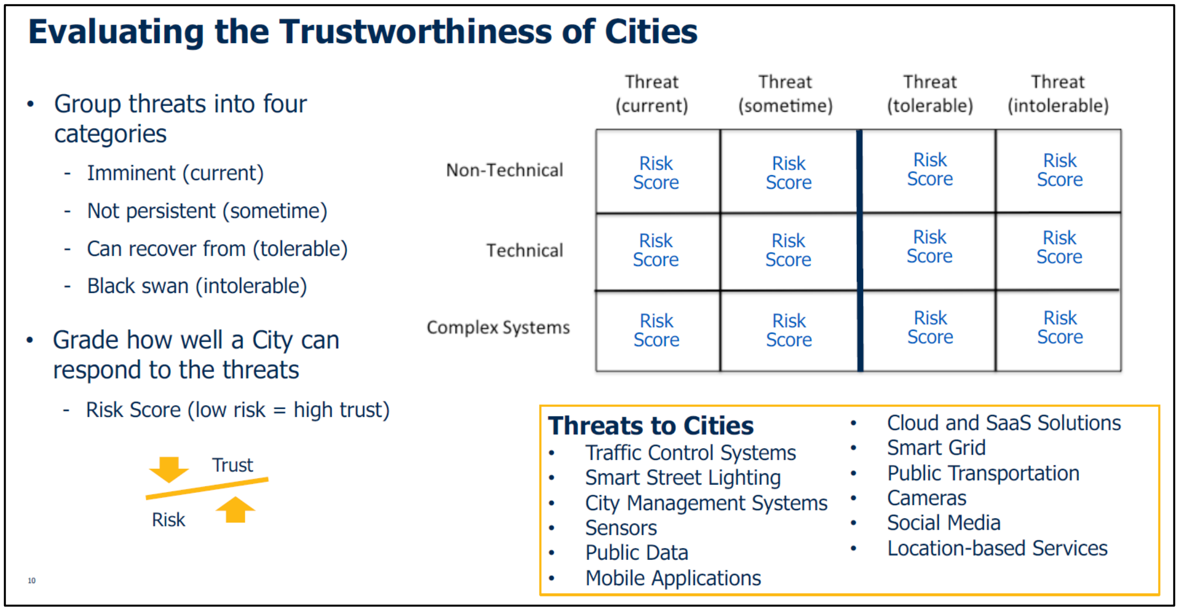
[141] See also this perspective on edge computing: Industrial Internet Consortium Press Release and embedded White Paper, "The Industrial Internet Consortium Publishes Edge Computing in IIoT White Paper," June 18, 2018 https://www.iiconsortium.org/press-room/06-18-18.htm

[142] Source: NIST Special Publication 500-325 op. cit.

[143] See supra footnote 71 and figure 8; and infra footnote 220.

> *of operating securely, reliably, and accountably /…/ Being prepared is key to preventing bigger problems and chaos. Cyber security problems are all around us, and smart cities will be wide open to cyber-attacks. This is a real and immediate danger. It's only a matter of time before cyber-attacks on city services and infrastructure happen. The more technology a city uses, the more vulnerable to cyber-attacks it is, so the smartest cities face the highest risks."*[144]

Dr. Loper proposes to classify the threats to Smart Cities in four categories according to time and tolerability characteristics, i.e., current (or imminent), sometime (not persistent), tolerable (can recover from) and intolerable (e.g., black swan[145] events); and to grade how well the Smart City is able to respond to these threats in three risk areas, i.e., non-technical (management, training and education, and best practices); technical (software development, cyber-attacks, and data and devices); and complexity, i.e., complex interconnection of diverse systems (cascade effects and exposure to "normal accidents"[146]). Her evaluation matrix is presented in Figure 12 below:



Evaluating the Trustworthiness of Cities

- Group threats into four categories
  - Imminent (current)
  - Not persistent (sometime)
  - Can recover from (tolerable)
  - Black swan (intolerable)
- Grade how well a City can respond to the threats
  - Risk Score (low risk = high trust)

Trust
Risk
10

	Threat (current)	Threat (sometime)	Threat (tolerable)	Threat (intolerable)
Non-Technical	Risk Score	Risk Score	Risk Score	Risk Score
Technical	Risk Score	Risk Score	Risk Score	Risk Score
Complex Systems	Risk Score	Risk Score	Risk Score	Risk Score

Threats to Cities

- Traffic Control Systems
- Smart Street Lighting
- City Management Systems
- Sensors
- Public Data
- Mobile Applications
- Cloud and SaaS Solutions
- Smart Grid
- Public Transportation
- Cameras
- Social Media
- Location-based Services

Figure 12: Matrix for Evaluating the Trustworthiness of Cities[147]

[144] Margaret L. Loper, "Trusting Smart Cities: Risk Factors and Implications," Small Wars Journal, June 19, 2018 http://smallwarsjournal.com/jrnl/art/trusting-smart-cities-risk-factors-and-implications

[145] See Nassim Nicholas Taleb, "The Black Swan: The Impact of the Highly Improbable," The New York Times, April 22, 2007 https://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html

[146] "*Normal Accidents analyzes the social side of technological risk. Charles Perrow argues that the conventional engineering approach to ensuring safety--building in more warnings and safeguards--fails because systems complexity makes failures inevitable. He asserts that typical precautions, by adding to complexity, may help create new categories of accidents."* Source: https://press.princeton.edu/titles/6596.html

[147] Margaret L. Loper, "Trusting Smart Cities: Risk Factors and Implications," presentation at the Mad Scientist Conference: Installations of the Future, hosted by the Office of the Assistant Secretary of the Army for Installations, Energy and Environment (OASA (IE&E)), with Georgia Technology Research Institute

Regardless of how vital technology (connectivity) is, it is “just one layer of many in the smart city ecosystem.”[148]

What matters is how (including how securely, privately, etc.), and to what extent, technology, in its many components, can power and generate the so-called digital transformation throughout the Smart City ecosystem for the citizens’ benefit.

George Westerman, a principal research scientist with the MIT Initiative on the Digital Economy, unambiguously makes this point in a recent piece for the MIT Sloan Management Review:

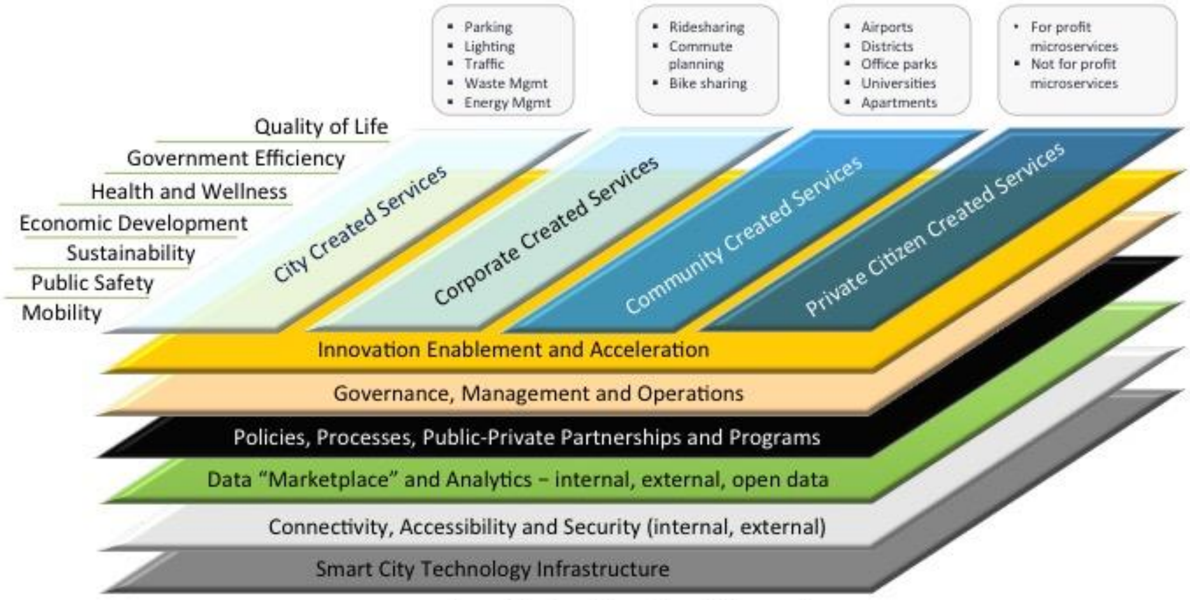
> *”As sexy as it is to speculate about new technologies such as AI, robots, and the internet of things (IoT), the focus on technology can steer the conversation in a dangerous direction. Because when it comes to digital transformation, digital is not the answer. Transformation is. Technology doesn’t provide value to a business. It never has (except for technology in products). Instead, technology’s value comes from doing business differently because technology makes it possible /…/ IoT is not about RFID tags — it’s about radically synchronizing operations or changing business models.”*[149].

The many layers (tangible and intangible) making up the Smart City ecosystem are shown in Figure 13 below:

(GTRI) and the U.S. Army Training and Doctrine Command (TRADOC), GTRI, Atlanta, Georgia, June 19, 2018. The presentation is available on the Thought Leadership section of the CDAIT website: https://cdait.gatech.edu/thought-leadership. The list of threats in the “Threat to Cities” box is from Cesar Cerrudo, “An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks,” IOActive White Paper, 2015, (“key technologies and systems that together make up the smart city’s complex attack surface,” pp. 12-13), available at https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf

[148] Benson Chan, “Building the smart city: 8 things that matter -- Tomorrow’s cities are built by smart city ecosystem architects today. To be effective, these architects must expand their perspectives, assume new roles, and work strategically,” Network World, March 27, 2018 https://www.networkworld.com/article/3266288/internet-of-things/building-the-smart-city-8-things-that-matter.html

[149] George Westerman, “Your Company Doesn’t Need a Digital Strategy,” in the MIT Sloan Management Review, Spring 2018 Issue Volume 59, Issue # 3, March 13, 2018 https://sloanreview.mit.edu/article/your-company-doesnt-need-a-digital-strategy/


Parking
Lighting
Traffic
Waste Mgmt
Energy Mgmt
Ridesharing
Commute planning
Bike sharing
Airports
Districts
Office parks
Universities
Apartments
For profit microservices
Not for profit microservices
Quality of Life
Government Efficiency
Health and Wellness
Economic Development
Sustainability
Public Safety
Mobility
City Created Services
Corporate Created Services
Community Created Services
Private Citizen Created Services
Innovation Enablement and Acceleration
Governance, Management and Operations
Policies, Processes, Public-Private Partnerships and Programs
Data "Marketplace" and Analytics – internal, external, open data
Connectivity, Accessibility and Security (internal, external)
Smart City Technology Infrastructure

Source: StrategyofThings.io/smart-city-ecosystem

Figure 13: Smart City Ecosystem Framework[150]

In the following section, five Smart City use cases will be reviewed through the EPIC screen, i.e., Municipal Services Management; Utilities; Public Safety; Transportation; and Healthcare.

A graphic outline of EPIC is presented in Figure 14.

[150] Source: Benson Chan, "Building Smart Cities: Eight Things That Matter," Blog, March 28, 2018 https://strategyofthings.io/smart-city-ecosystem-architects

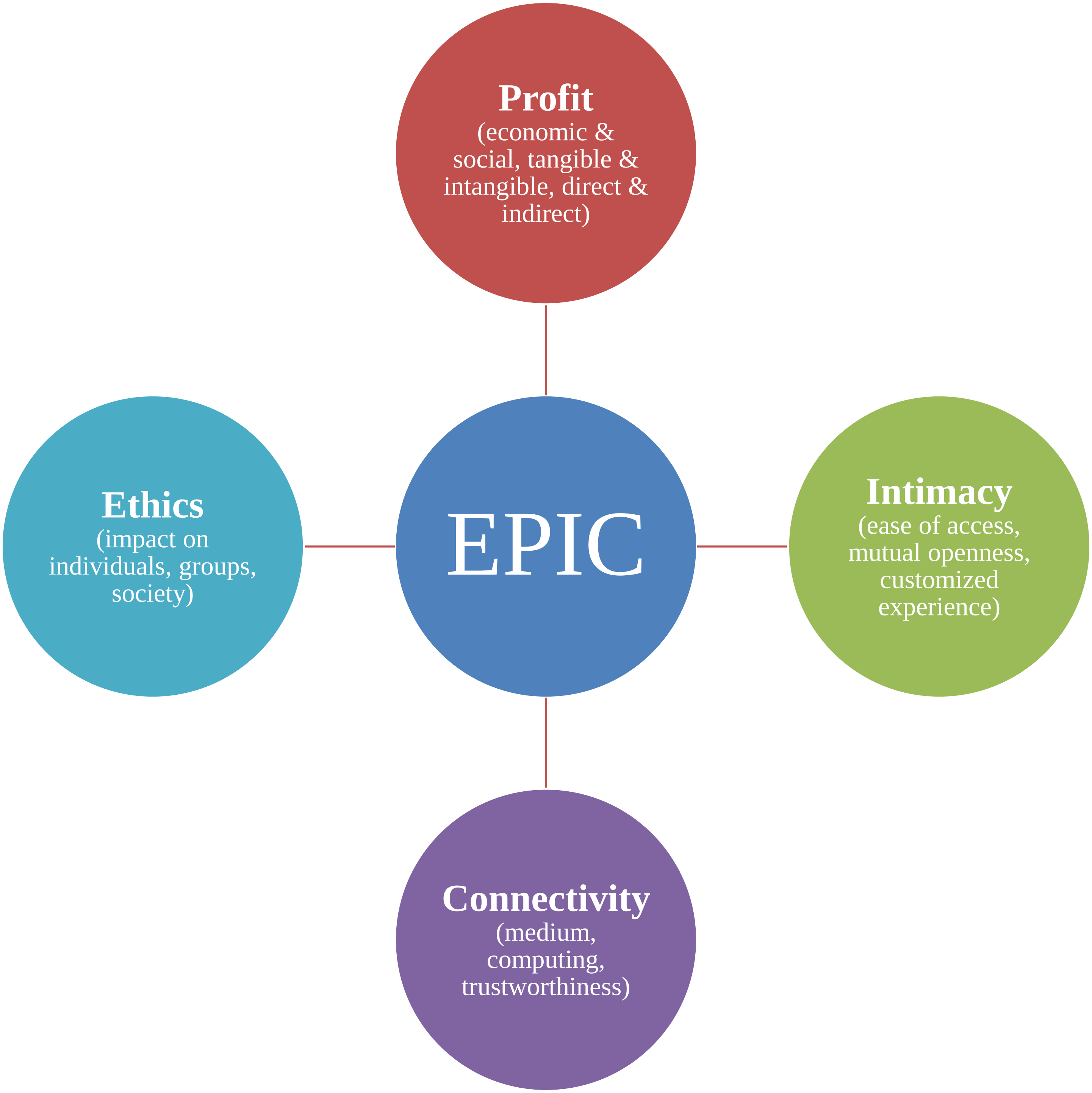

Profit
(economic & social, tangible & intangible, direct & indirect)
Ethics
(impact on individuals, groups, society)
EPIC
Intimacy
(ease of access, mutual openness, customized experience)
Connectivity
(medium, computing, trustworthiness)

Figure 14: EPIC screen for IoT development[151]

4.4 USE CASES

4.4.1 Municipal Services Management

As noted earlier in this paper (Section 2.4.1), Pierce and Andersson's 2017 study[152] shows that the spectrum of concerns surrounding Smart City initiatives is wide and ranges from technical to governance to managerial challenges.

IoT technologies may help overcome some of these hurdles.

By utilizing an IoT-supported approach, employees will be more productive, and, consequently, in a position to generate operational efficiencies.

Extending this concept to other stakeholders can lead to a streamlined supply chain that is not only efficient but also promotes partner collaboration, a solid source of innovation[153].

Promoting intimacy through easy access, mutual openness and customized experience without jeopardizing the citizens' privacy and other ethical considerations[154], developing enabling policies and encouraging technology awareness (capabilities and limitations) are indispensable action items on the critical path of Smart City deployment.

Success begets success: The adoption of IoT technologies will be accelerated when they bring about an enhanced citizen experience.

By leveraging IoT concepts to interface with the community, municipal services can be offered cost-effectively, faster, in more places, and with more customized interactions than previously possible.

However, regardless of the technological and other achievements, effectively and efficiently addressing the various trustworthiness elements is of paramount importance.

[151] Source: Georgia Tech Center for the Development and Application of Internet of Things Technologies (CDAIT)

[152] Pierce, P., & Andersson, B. (January 2017), op. cit.

[153] See Charlie Covert, "IoT and the Future of Consumer Products Manufacturing," UPS Longitudes, May 31, 2017 https://longitudes.ups.com/iot-and-the-future-of-consumer-products-manufacturing/

[154] See for example Anthony Burke, "Three scenarios show we have to think carefully about ethics in designing smart cities," The Conversation, March 16, 2018 https://theconversation.com/three-scenarios-show-we-have-to-think-carefully-about-ethics-in-designing-smart-cities-91213

Ethics	Profit	Intimacy	Connectivity
• Equity of access, e.g., enhanced services provided to vulnerable populations[155] without any discrimination	• Economic: More efficiently meeting citizens' needs • Social: Reaching out to broader footprint of the population	• Customized and remote delivery of services (i.e. not having to go to a central office) should reduce inconvenience and expenses • Free and easy access to data will boost confidence in system	• Proper design/ implementation can use the same communications infrastructure for multiple municipal services, enhancing efficiency. • Attention to trustworthiness is critical

Table 4: EPIC Screen for Municipal Services Management

4.4.2 Utilities

According to the US Department of Energy, today's electricity system is 99.97% reliable, yet still allows for power outages and interruptions that cost Americans at least $150 billion/year (approximately $500 for every man, woman and child)[156]. Even a 1% reduction in interruption would result in over $1 billion in annual savings.

Ethics	Profit	Intimacy	Connectivity
• Able to protect vulnerable groups (e.g. ventilator-dependent seniors)	• Economic: Billions of dollars saved by reducing blackouts • Social: Ability to monitor water delivery can save lives and improve public health, protect the environment	• Customized use of resources can reduce cost and inconvenience to individuals, improve delivery to critical groups	• Widespread sensor network can be supported by low-bandwidth connections (Low-Power Wide Area Network) • Protecting network integrity is a matter of national security

Table 5: EPIC Screen for Utilities

[155] *"Vulnerable Population"* is defined in Section 2.4.3 (footnote 51)

[156] Source of data: "The Smart Grid: An Introduction," 2008, p.5, a report prepared for the U.S. Department of Energy by Litos Strategic Communication under contract No. DE-AC26-04NT41817, Subtask 560.01.04 https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf

Examples

1. Cleveland, Ohio overhauled its water department using smart monitoring to reduce waste, remove redundancies and better manage resources. The initiatives generated a new $14 million annual revenue stream and allowed the city to streamline billing, reduce errors and inefficiencies (Cleveland Plain Dealer, Cleveland Mayor Frank Jackson says water department overhaul could mean no rate hikes for 5 years, January, 2013)
2. In Yokohama, Japan, Building Energy Management Systems (BEMS) are installed for commercial buildings to optimize power control and reduce peak consumption by 20%. (Green Future Solutions, Yokohama Smart City Project Demonstrates Energy Management and Demand Response in Smart Cities, October, 2013).

4.4.3 Public Safety

In the movie "Minority Report" the police force of the future fought crime by using "psychics" and super-intelligent data to reduce and/or prevent crime. While the state-of-the-art is not quite there yet, significant progress is being made in leveraging predictive crime trends to reduce crime.

IoT plays a critical role in revolutionizing law enforcement by leveraging data from weather patterns, public transit movements, social media sensors and gunshot sensors to predict crime. The city of San Francisco uses gunshot sensors in high crime neighborhoods to identify the sound of gunfire and can dispatch police officers before anyone calls 911. This technology has reduced homicides by as much as 20% in some localities[157].

When it comes to public safety, municipalities must not sacrifice citizen intimacy and ethical responsibility (according to EPIC) for the sake of efficiency. Lukewarm attention to these issues will slow down IoT technology adoption.

Ethics	Profit	Intimacy	Connectivity
• Equity: safety must be provided to all citizens • A danger of violation of privacy depending on system implementation and usage	• Better situational awareness, faster response times, and improved traffic navigation can create tangible improvements in survival rates, property protection, etc., creating both economic and social benefit	• Medical personnel can tailor the response to the patient • IoT can ease communication with public safety dispatchers, etc. • Stakeholder openness is key	• High-availability, real-time connectivity crucial in life-or-death situations • Struggle between full data vs. ability to process/ digest data in real time • Trust is foundational

Table 6: EPIC Screen for Public Safety

[157] Philip Tracy, "How Industrial IoT is Improving Public Safety", RCRWireless News, September 1, 2016 https://www.rcrwireless.com/20160901/big-data-analytics/iiot-public-safety-tag31-tag99

Examples

1. Civilian drones have been used to save at least 59 people in 18 different incidents around the world since 2013. It is now predicted that a drone is saving nearly one person's life a week on average.[158]

2. See also Project Greenlight in Detroit[159], and more generally this recent observation regarding solving key public safety challenges:

   "Communities are beginning to see the value of security solutions powered by collaborative IoT. Integrating systems is a big trend, as well as data analytics, setting up some big opportunities. In 2018, the industry value (globally) has been estimated at $100 billion or more."[160]

4.4.4 Transportation

According to the U.S. Census Bureau,

> *"By 2060, the United States is projected to grow by 78 million people, from about 326 million today to 404 million*."[161]

This growth will strain urban infrastructure across all transportation modes. In 2016, 28% of the US Green House Gas (GHG) emissions were created from transportation (cars, trucks, commercial aircraft, rail, ships and other).[162]

[158] Dan Reisinger, "Here's How Many Lives Drones Have Saved Since 2013", Fortune, March 14, 2017 http://fortune.com/2017/03/14/drones-save-live

[159] Project Greenlight Detroit website: http://www.greenlightdetroit.org/about/

[160] Project Greenlight description and comment on solving key public safety challenges can be found here: Justin Slade, "Improving public safety with collaborative IoT security solutions," Microsoft Website, May 18 2018 https://enterprise.microsoft.com/en-us/articles/industries/government/improving-public-safety-with-collaborative-iot-security-solutions/

[161] U.S. Census Bureau Press Release, "Older People Projected to Outnumber Children for First Time in U.S. History," March 13, 2018 https://www.census.gov/newsroom/press-releases/2018/cb18-41-population-projections.html

[162] United States Environment Protection Agency (EPA) website: https://www.epa.gov/ghgemissions/sources-greenhouse-gas-emissions

Ethics	Profit	Intimacy	Connectivity
• Improved transportation efficiency would have widespread benefit; however, specific projects would need to be analyzed for untended consequences on sub-groups (economically, geographically, etc.)	• Self-driving cars allow reduction of transport cost and fuel consumption (positive impact on environment) + support underserved population (e.g. people with disabilities) – impact economic and social profit • Sensors as a service can be deployed in parking spaces in business districts • Parking availability sensors reduce time and travel for finding parking spaces	• Sensors for tracking commuting needs and historical patterns • Traffic data captured by sensors can be communicated to drivers • Direct traffic through alternate routes, open lanes, automated traffic lights (decrease traffic congestion) • Customized experience function of ubiquitous availability	• Sensors for tolling throughout roads and bridges • Efficient connectivity can enable optimization of toll pricing to account for traffic flow • Truck driving monitoring can help raise productivity

Table 7: EPIC Screen for Transportation

Examples

1. In Helsinki, Finland[163], fuel consumption has dropped 5%, customer satisfaction has increased 7%, driver performance has improved, and mechanical maintenance has become proactive by analyzing data from sensors installed in public areas.
2. New York's Citi Bike bicycle sharing service offset 2,145,628 pounds of carbon in the month of June 2017[164].

4.4.5 Healthcare

According to the United Nations, by 2050, two thirds of the world population will be urban, and many cities will have over 10 million inhabitants.[165]

At the same time, the population in those cities will be rapidly aging, which may make the insertion of Internet of Things technologies timely:

> *"The IoMT [Internet of Medical Things] might be the silver bullet for our communities to address a burdened healthcare system that will only be under more stress as our*

[163] Microsoft website (Customer Story), "Helsinki Bus Firm Cuts Fuel Use, Offers Improved Transport," February 16, 2015 https://customers.microsoft.com/en-us/story/helsinki-bus-firm-cuts-fuel-use-offers-improved-transp

[164] NYC Bike Share, Citi Bike, June 2017 Monthly Report, p.3 https://d21xlh2maitm24.cloudfront.net/nyc/June-2017-Citi-Bike-Monthly-Report.pdf?mtime=2017071909463

[165] United Nations, "World's population increasingly urban with more than half living in urban areas," July 10, 2014 http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

> *population continues to* age. By 2025, 1.2 billion of the 8 billion people on earth will be elderly; equivalent to the population *of India. Elderly people tend to have more healthcare issues, therefore increasing costs. So, as life expectancy rises, it is expected that healthcare costs will follow suit. IoMT can provide a better way to care for our elderly and has a tremendous potential to help deal with the rising costs of care. IoMT devices can help track vitals and heart performance, monitor glucose and other body systems, and activity and sleeping levels."*[166]

However enticing the promises on the horizon are, IoT adoption by the elderly is still slow and requires urgent and thorough investigation:

> *"Although a lot of work is being done on the technological aspects of smart homes, yet their [i.e., health and other ambient assisted living technologies,] adoption rate is very low mainly due to their disruptive nature and inherent conservativeness of the older people towards any new technology. Current research on IoT and smart homes point out towards the benefits of using such a system by the elderly along with a strong thrust in developing new underlying technologies and service. However, there is a lack of evidence of how the subjective opinion of the people can be influenced towards using these services/systems."*[167]

On other healthcare-related fronts, the ever-expanding ecosystem of IoT connected devices – from wheelchairs and walkers to wearable health monitors and sensors inside our bodies – presents new opportunities for solution providers through the storage, management, access, and analysis of massive amounts of data to improve patient care and control costs.[168]

Furthermore, IoT technologies are well suited to comply with the U.S. Drug Supply Chain Security Act (DSCSA), which outlines steps to build an electronic, interoperable system to identify and trace certain prescription drugs as they are distributed in the United States (to help prevent counterfeiting and theft). IoT solution providers will be able not only to offer tracking services but also additional services such as temperature of the environment being monitored as well as the package's location.[169]

[166] Bernard Marr, "Why The Internet Of Medical Things (IoMT) Will Start To Transform Healthcare In 2018," Forbes, January 25, 2018 https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#125580de4a3c

[167] Debajyoti Pal et al., "Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective," IEEE Access, 0.1109/ACCESS.2018.2808472, March 15, 2018 version, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8300511

[168] AT&T Business Editorial Team, "How healthcare organizations are innovating with Edge-to-Edge technologies," AT&T website https://www.business.att.com/learn/operational-effectiveness/how-healthcare-organizations-are-innovating-with-edge-to-edge-technologies.html

[169] Verizon website, "Healthcare is in the midst of an IoT boom," January 31, 2017 https://www.verizon.com/about/news/healthcare-midst-iot-boom

Ethics	Profit	Intimacy	Connectivity
• Health data privacy is imperative to protect against all kinds of malicious use including improper discrimination based on health data (compliance with HIPAA and HITECH Act) • Equity: Better access to healthcare for underserved groups	• Can increase effectiveness and efficiency of health care, providing substantial economic and social benefits • Platform marketplace for health data for cost-effective collaboration • Social: Analysis to predict epidemics and dangerous pollution levels • Social: IoT technologies can help prevent drug counterfeiting and theft	• Virtual closeness via telehealth and telemedicine • Precision (personalized) medicine • Bidirectional and direct information exchange between city and citizens increase effectiveness of health programs, e.g., vaccinations	• Various sensors from basic telecare alarms to more sophisticated remote patient monitoring for chronic diseases • Tight cybersecurity is key to ensure privacy

Table 8: EPIC Screen for Healthcare

Examples

1. In Barcelona, the Telecare service[170] looks after more than 70,000 elderly and disabled citizens by proactively checking on them using sensors.

2. In 2015, the United Arab Emirates (UAE) approved a cabinet-backed plan to establish a unified national health database to connect all hospitals and clinics for accessing a patient's medical history, ailments, surgeries and tests conducted. Unifying data means patients can move across hospitals and clinics freely.[171]

3. Children with asthma in the Rochester City School District who received a combination of telemedicine support and school-based medication therapy were almost half as likely to need an emergency room or hospital visit for their asthma, according to the University of Rochester Medical Center (URMC)[172]

4. According to Belgium-based company i-SCOOP,

   "The usage of the IoT in healthcare (the industry, personal healthcare and healthcare payment applications) has sharply increased across various specific Internet of Things use cases."[173]

[170] Paul Burstow, "Telecare: The UK should learn from Barcelona's example," The Guardian, March 16, 2015 https://www.theguardian.com/social-care-network/2015/mar/16/telecare-uk-barcelona-paul-burstow

[171] Smart City, "Smart Healthcare Solutions for Smart Cities," August 5, 2017 https://www.smartcity.press/smart-healthcare-for-smart-cities/

[172] University of Rochester Medical Center Press Release, "For City Kids with Asthma, Telemedicine and In-School Care Cut ER Visits in Half," January 8, 2018, https://www.urmc.rochester.edu/news/story/5216/for-city-kids-with-asthma-telemedicine-and-in-school-care-cut-er-visits-in-half.aspx

[173] I-SCOOP, "Internet of Things (IoT) in healthcare: benefits, use cases and evolutions," https://www.i-scoop.eu/internet-of-things-guide/internet-things-healthcare/

4.5 Conclusions And Next Steps

When used within the context of a city, IoT technologies should not be built or marketed based on what makes a city smarter, but rather on what makes citizens smarter and more aware; in short, their development and deployment must be citizen-centric.

IoT implementations for communities will be successful to the extent they are tightly aligned with users' conditions and needs, and reflect a value proposition that is straightforward.

The proposed EPIC screen provides a useful guide to evaluate an IoT project through four simple but crucial questions:

1) Does it conform to generally accepted moral and social norms (ethics)?

2) Does it generate attractive economic and social benefits (profit)?

3) Does it foster a close relationship between the stakeholders (intimacy)? and

4) Is it delivered through effective technological means (connectivity)?

Moving forward, it is critical to evaluate the "goodness of fit" of a business model (be it traditional or other new monetization method) via the use of trials rather than a "big bang" implementation of what seems to be a good idea but has no measurable evidence of fit. Designing these trials to be representative and scalable will be essential.

Municipalities implementing IoT projects should engage vendors and internal IT/OT staff on a "proofs of concept" basis. This way, data can be collected to support evidence-based goals for value achievement and usefulness. These "proofs of concept" must be well designed, with well-defined scopes, time limits, budget, functionalities under test, roles of participants, and agreed-upon success criteria. Taking these steps will help assure value attainment as well as usefulness for stakeholders and users.

5 QUESTION 4: IoT ROADMAPS

WHAT POSSIBLE ROADMAPS CAN LEAD TO THE IoT REVOLUTION BECOMING THE IoT OF THE FUTURE?

5.1 INTRODUCTION

McKinsey estimates that 127 new devices connect to the internet every second[174] and global information provider IHS Markit projects the number of connected Internet of Things (IoT) devices to grow globally to more than 31 billion in 2018.[175]

With the deployment of 5G technologies, the period of 2020 to 2025 will witness IoT technological improvement, adoption and acceleration[176].

The number of cars will double worldwide and reach the two billion mark by 2040, thus increasing fuel consumption and the amount of carbon dioxide in the atmosphere. New materials (biofuels, ethanol, etc.) and emerging technologies (auto/ride sharing, autonomous/smart vehicles, etc.)[177], sensors and actuators, machine-driven software and networking technologies will continue to improve to solve transportation issues. Similar ameliorations will permeate all other market verticals.

Enhanced mobile broadband and mission critical control-solving latency, spectrum, connectivity, capacity, density and energy efficiency will facilitate the emergence of innovative solutions that we can barely imagine today. New regulations and standards will eventually target developing and established markets.

Most researchers point to data-driven focus on IT connectivity, e-governance, public transportation, water, power, sanitation/solid waste management and urban mobility as definitional characteristics of a Smart City. Integrated IT management and data accessibility

[174] Source: Mark Patel, Jason Shangkuan, and Christopher Thomas, "What's New with the Internet of Things", May 2017, https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things

[175] Source: IHS Markit Press Release (Business Wire), "IHS Markit Identifies Top Trends Driving the Internet of Things in 2018 and Beyond", February 1, 2018, https://www.businesswire.com/news/home/20180201005203/en/IHS-Markit-Identifies-Top-Trends-Driving-Internet. A roundup of current IoT forecasts can be viewed here: Louis Columbus, "2017 Roundup of Internet of Things Forecasts", December 10, 2017.

[176] See: Research and Markets Press Release, "5G Technology and Solutions for IoT Markets, 2025", September 15, 2017, https://www.prnewswire.com/news-releases/5g-technology-and-solutions-for-iot-markets-2025-300520254.html, and 5G Americas, "LTE Progress Leading to the 5G Massive Internet of Things", December 2017, http://www.5gamericas.org/files/8415/1250/0673/LTE_Progress_Leading_to_the_5G_Massive_Internet_of_Things_Final_12.5.pdf

[177] The World in 2050 (The Real Future of Earth) – Full BBC Documentary 2017, http://www.documentarytube.com/videos/the-world-in-2050-the-real-future-of-earth-full-bbc-documentary-hd and see Matthew Nitch Smith, "The number of cars will double worldwide by 2040", April 20, 2016, http://www.businessinsider.com/global-transport-use-will-double-by-2040-as-china-and-india-gdp-balloon

are key. It is, therefore, not surprising that the United Nations E-Government Survey released in 2016 reports that the number of Chief Information Officers grew from 29 in 2008 to 111 in 2016, representing 58% of the United Nations member states[178].

Additionally, the use of Open Government Data among UN member states, which refers to “government information proactively disclosed and made available online for everyone’s access, reuse and redistribution without restriction”, has sharply increased from 46 nations in 2014 to 106 in 2016 as reported in the United Nations E-Government Survey 2016. These trends would tend to suggest that digital administration is becoming more pervasive around the world, which could provide a favorable environment for the advent of Smart Cities.

One might assume that the rate of adoption of Smart City-related technologies would vary greatly between countries at different stages of economic development. While it is true that the overall adoption of technology within developing countries is lower than within developed countries, in some cases, Smart City-centered technologies adoption is faster in the former than in the latter.

For example, Ghana has piloted an electronic land registry based on Blockchain technology[179], thanks to its ability to address government corruption through transparency and immutable record keeping. Similarly, the affordability and widespread use of mobile technology has allowed Mozambique to engage citizens through SMS and mobile applications to report waste management needs and illegal dumping[180].

These examples and the previously mentioned trends around integrated IT Management and Open Government Data could perhaps be seen as harbingers of Smart Cities.

Likewise, a major driver of remote surgery is, in fact, not for a local doctor to stay at home while he or she consults across town, but to enable remote and disadvantaged areas the opportunity for healthcare solutions otherwise not available.

Data exchange, coupled with the ability to perform remote monitoring and control, may induce the emergence of new business models for developing countries and offer additional revenue streams for local businesses[181].

However, the Forrester graphic below (Figure 15) points out how the various technology components continue to evolve at differing speeds and trajectories.

[178] UN E-Government Survey 2016 https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2016

[179] Bitland's African Blockchain Initiative: Putting Land on The Ledger, Forbes Apr 5, 2016, https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#40865d767537

[180] The United Nations E-Government Survey 2016 op. cit.

[181] See International Telecommunication Union (ITU), “Harnessing the Internet of Things for Global Development”, January 2016, https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

This section reviews the IoT roadmap within the Smart City context through the lenses we have used above, i.e., municipal services management, utilities, public safety, transportation and healthcare, and reflects on the integration requirements specific to the Smart Cities.

The analysis starts by singling out two indispensable elements ("sine qua non") on which rests the successful Smart City deployment, i.e., privacy and IoT device connection.

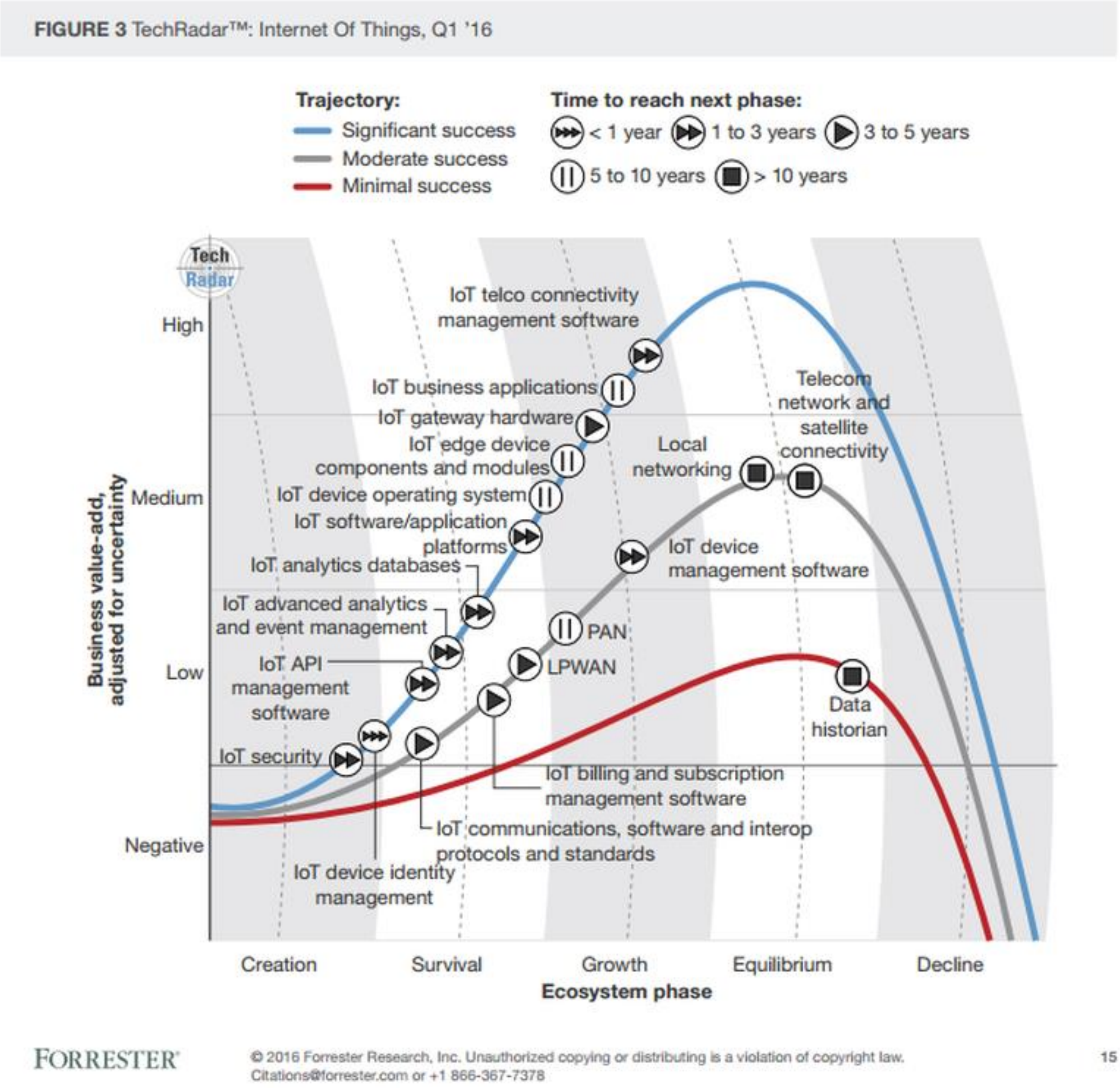


FIGURE 3 TechRadar™: Internet Of Things, Q1 '16

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Figure 15: Business value-add vs. ecosystem phase[182]

[182] 2016. Forrester graphic can be found in Larry Dignan, "Internet of things security years away from being fully baked, says Forrester" January 26, 2016, https://www.zdnet.com/article/internet-of-things-security-years-away-from-being-fully-baked-says-forrester/

5.2 PRIVACY AS THE CORNERSTONE OF CITIZEN INTERACTION

Smart Cities is one of the significant drivers fueling the rise of connected devices across the private and public sectors. Juniper Research predicts that by 2021, Smart Cities will have saved $19 billion through efficiencies driven by IoT. [183] In March 2018, it was reported that:

> *"Worldwide spending on the technologies that enable Smart Cities is forecast to reach $80 billion in 2018, according to the International Data Corporation's (IDC) latest study. In the first release of its Worldwide Semiannual Smart Cities Spending Guide, over five years that total will reach $135 billion by 2021."*[184]

Becoming a "Smart City" is a long-term transformation that requires assessing and addressing the security and privacy concerns of IoT deployment. Security issues are discussed in Section 3.2 IoT Security*.*

Privacy is a domain of growing concern in the Internet of Things space[185] and within Smart Cities in particular as they become laden with a wide range of sensors that can capture in some form or another details of the citizens' life.

It is therefore not surprising that Smart Cities-related bills recently introduced in the 115th United States Congress (2017-2018), e.g., Smart Cities and Communities Act of 2017 (H.R. 3895[186] and S. 1904[187]), and the "Smart Technology for Resilient, Efficient, Economic and Reliable Transportation in Cities and Communities Act" or the "STREET Act" (H.R. 4151[188]) have privacy safeguard as one of their core tenets.

These efforts notwithstanding, dealing with privacy within a Smart City may need new approaches beyond legislation:

> *"Although governments already collect lots of data on their citizens, it's becoming clear that current privacy laws aren't going to be enough to deal with the realities of what most of these visions propose — data collection on a scale that far surpasses what's happening today. 'I think in some ways what we're facing here is a situation where none of this is very much like anything we've seen before,' says David Murakami Wood, an associate professor at Queens University, who studies*

[183] Juniper Research, "Smart Cities on the Faster Track to Success", https://www.juniperresearch.com/document-library/white-papers/smart-cities-on-the-faster-track-to-success

[184] Cynthia S. Artin, "From $80 Billion to $135 Billion: Global Smart City Spending Still Climbing", IoT Evolution, March 2, 2018, http://www.iotevolutionworld.com/iot/articles/437272-from-80-billion-135-billion-global-smart-city.htm

[185] In the IoT privacy domain, the work of the "Internet of Things Privacy Forum", which, according to its website "is an international nonprofit think/do tank producing guidance, analysis, research and best practices for industry and government to reduce privacy risk by innovating responsibly in the domain of connected devices" needs to be highlighted; see https://www.iotprivacyforum.org/ and Gilad Rosner and Erin Kenneally, "Privacy and the Internet of Things – Emerging Framework for Policy and Design," Center for Long-Term Cybersecurity, (CLTC), UC Berkeley, June 7, 2018 https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf

[186] Accessible at: https://www.congress.gov/bill/115th-congress/house-bill/3895

[187] Accessible at: https://www.congress.gov/bill/115th-congress/senate-bill/1904

[188] Accessible at: https://www.congress.gov/bill/115th-congress/house-bill/4151

> *surveillance in cities. He's not the only one who's skeptical that the law can keep up."*[189]

In this regard, the variety of perspectives conveyed ahead of and during the May 22, 2018 hearing on "Internet of Things legislation", i.e., regarding the ''State of Modern Application, Research, and Trends of IoT Act'' or the ''SMART IoT Act'', before the Subcommittee on Digital Commerce and Consumer Protection of the U.S. House Energy and Commerce Committee demonstrates that there is no consensus on the need for and the role of regulation when it comes to privacy, security, and physical safety risks of the Internet of Things[190].

In a January 2018 opinion article in the *Toronto Star* about the building of an experimental digital urban neighborhood "from the internet up" in an area of the Toronto waterfront that is no longer used, University of Toronto Emeritus Professor Andrew Clement expresses his concern that "individually and collectively, Canadians are rapidly losing effective control of their digital lives." He outlines five criteria for protecting privacy and other related rights, which could altogether be viewed as a potential blueprint for digital governance of Smart Cities:

1. All data collection should be anonymous by default;
2. All data derived from individuals must comply with privacy laws;
3. Software that accesses data gathered should be available under a free open source license in a public repository;
4. Basic digital services should be accessible and affordable for all the neighborhood residents; and
5. Security of the data, software and physical infrastructure should be maintained by appropriately robust means, and breaches immediately reported[191].

The city of Barcelona is already integrating this type of framework in its experiments in open democracy and data protection. Everything Barcelona has developed is open source, and all the code is posted on Github[192]. Dr. Francesca Bria, Barcelona's Chief Technology and Digital Innovation Officer, explains how Barcelona is "reversing the smart city paradigm":

> *"In cities, more than 90 per cent of the data we use today didn't exist three years ago," says Bria. "And this is just the beginning: now with 5G, with the internet of*

[189] See Braga, M., "Welcome to the neighbourhood. Have you read the terms of service? - How we think about privacy today might not be the best way to deal with data collection in a Smart City," CBC News, January 16, 2018, http://www.cbc.ca/news/technology/smart-cities-privacy-data-personal-information-sidewalk-1.4488145

[190] See https://energycommerce.house.gov/news/press-release/subdccp-examines-smart-iot-act/) and, for example, EPIC (Electronic Privacy Information Center)'s statement dated May 21, 2018 ahead of the hearing https://epic.org/testimony/congress/EPIC-HEC-IoTLeg-May2018.pdf. See also: Kayla Matthews, "Smart IoT Act Approved, Leaves out Security Concerns," Central IoT, June 21, 2018 https://www.iotcentral.io/blog/smart-iot-act-approved-leaves-out-security-concerns

[191] Clement, A., "Sidewalk Labs' Toronto waterfront tech hub must respect privacy, democracy," The Toronto Star, January 12, 2018, https://www.thestar.com/opinion/contributors/2018/01/12/sidewalk-labs-toronto-waterfront-tech-hub-must-respect-privacy-democracy.html

[192] See https://github.com/AjuntamentdeBarcelona

> *things, with artificial intelligence — this is the very beginning of a big disruption, what the industry call 4.0. We want to move from a model of surveillance capitalism, where data is opaque and not transparent, to a model where citizens themselves can own the data"*[193]

Surveillance Capitalism is a concept that has been popularized by Harvard Business School Emeritus Professor Shoshana Zuboff:

> *"Surveillance capitalism renders behavior so that it can be parsed as observable, measurable units. Once it's rendered as behavior it is turned into data and that's the data that I call 'behavioral surplus'. These data are subjected to sophisticated analyses to manufacture 'prediction products,' and are then sold into what I call new 'markets in future behavior.' Huge revenues flow from these new markets. The logic of this new capitalism is that we are raw material resources."*[194]

In collaboration with the city of Amsterdam, Barcelona is also leading DECODE ((DEcentralised Citizen-owned Data Ecosystems)[195], a Europe-wide consortium funded by the European Union's Horizon 2020 Programme, which aims to explore how to build a data-centric digital economy where data that is generated and gathered by citizens, the Internet of Things (IoT), and sensor networks is available for broader communal use, with appropriate privacy protections. Dr. Bria, DECODE's project lead, emphasizes that, with this new data governance and identity management,

> *"Citizens can decide what kind of data they want to keep private, what data they want to share, with whom, on what basis, and to do what, this is a new social pact — a new deal on data."*[196]

Benjamin Franklin reminded fire-threatened Philadelphians in 1735 [197] "an ounce of prevention is worth a pound of cure." Franklin's prescient partiality toward prevention over cure (interestingly enough in a safety context) may be perfectly suited for the protection of privacy.

Privacy by Design (PbD), a term coined by Dr. Ann Cavoukian[198], is arguably about solving privacy problems before they exist and increasingly understood as part and parcel of an effective privacy protection strategy. Guided by the requirements of the European Union

[193] Thomas Graham, "Barcelona is leading the fightback against smart city surveillance", Wired (UK), May 18, 2018, http://www.wired.co.uk/article/barcelona-decidim-ada-colau-francesca-bria-decode

[194] See Lance Farrell, "Shoshana Zuboff: Rendering reality and cash cows," Science Node, October 17, 2017 https://sciencenode.org/feature/shoshana-zuboff,-part-two-rendering-reality.php, and a related article Shoshana Zuboff, "The Secrets of Surveillance Capitalism," Frankfurter Allgemeine Zeitung, March 5, 2016, http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html?printPagedArticle=true#pageIndex_0,

[195] Information on the project can be found here: https://decodeproject.eu/what-decode

[196] Thomas Graham, op. cit.

[197] Benjamin Franklin's text of this letter for the February 4, 1735 issue of The Pennsylvania Gazette can be found here: https://founders.archives.gov/documents/Franklin/01-02-02-0002

[198] See https://www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf

General Data Protection Regulation (GDPR)[199], it might become the keystone of Smart Cities' privacy strategy:

> *"According to Jorge Ortega, a lawyer from Barcelona specializing in data protection, and president of the expert committee of ANF (Data Protection Certification Authority) in Spain, 'City councils are responsible for all data collected by all IoT devices in public spaces, and the use of that data. If a light sensor detects the movement of cars entering or leaving a parking garage, and therefore the movement of its residents, their privacy needs to be protected by default.' He goes further: 'Privacy by design is mandatory when collecting data [on smart cities services], and cities cannot waive responsibility, and expect others to pick it up. They need to make sure the IoT devices installed on the streets comply with the regulation.'"*[200]

The general *seven PbD foundational principles* included in an October 2010 Resolution[201] passed unanimously by the regulators at the *International Conference of Data Protection Authorities and Privacy Commissioners,* which recognized Privacy by Design as an essential component of fundamental privacy are listed below:

1. Proactive not Reactive: Preventative, not Remedial;
2. Privacy as the Default setting;
3. Privacy Embedded into Design;
4. Full Functionality: Positive-Sum, not Zero-Sum;
5. End-to-End Security: Full Lifecycle Protection;
6. Visibility and Transparency: Keep it Open;
7. Respect for User Privacy: Keep it User-Centric.

These seven principles are effectively complemented by *eight privacy design strategies* proposed by the European Union Agency for Network and Information Security (ENISA)[202]:

1. Minimize (personal data processed restricted to the minimal amount possible)[203];
2. Hide (concealed from plain view to achieve unlinkability and unobservability);
3. Separate (distributed personal data in separate compartments whenever possible);
4. Aggregate (at the highest level with the least possible detail while still remaining useful);

[199] EU General Data Protection Regulation (GDPR) portal: https://www.eugdpr.org/

[200] See Pablo Valerio, "Europe's GDPR Slaps Data Collected by Cities," March 20, 2018 https://citiesofthefuture.eu/europes-gdpr-slaps-data-collected-by-cities-e9118fc648ab

[201] See https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

[202] See ENISA, "Privacy and Data Protection by Design – From Policy to Engineering", December 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

[203] The challenges around "data minimization" and other privacy protection issues for both lawyers and engineers are illustrated by Georgia Tech professors Peter Swire (law) and Annie Antón (software engineering) in their article on "Engineers and Lawyers in Privacy Protection: Can We All Just Get Along?" International Association of Privacy Professional (IAPP) Privacy Perspectives, January 13, 2014, https://iapp.org/news/a/engineers-and-lawyers-in-privacy-protection-can-we-all-just-get-along/

5. Inform (refers to transparency and openness);
6. Control (gives users the tools to exert their data protection rights, e.g., view, update and delete);
7. Enforce (in place through established governance structures);
8. Demonstrate (show compliance with policy and legal requirements).

PbD's framework embeds privacy into the design and architecture of IT systems and business practices. Applications for PbD include, but are not limited to[204]:

1. Closed Caption TV/Surveillance Cameras in Mass Transit Systems;
2. Biometrics Used in Casinos and Gaming Facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Devices & Communications;
5. Near Field Communications (NFC);
6. RFIDs and Sensor Technologies;
7. Redesigning IP Geolocation Data;
8. Remote Home Health Care;
9. Big Data and Data Analytics.

While the concrete implementation of PbD is still in an embryonic stage[205], the centrality and overwhelming importance of design in privacy can no longer be ignored as underscored in Northeastern University professor of law and computer science Woodrow Hartzog's recent book on *Privacy's Blueprint*:

> *"The most important decisions regarding your privacy were made long before you picked up your phone or walked out of your house. It is all in the design."*[206]

Michelle Dennedy, Jonathan Fox, and Tom Finneran in their *Privacy Engineer's Manifesto* stress the necessity of "privacy engineering" at this pivotal moment of IT innovation:

> *"We are yet at another pivotal moment given the ongoing and the ever accelerating pace of information technology innovation and consumerization. This acceleration is being driven by market demand – individuals who want new and different functionality from technology and uses of information – and market creation – enterprises and governments attempting to capitalize on new and expanding business models. The*

[204] Privacy by Design Primer – Information & Privacy Commissioner of Ontario (originally published in January 2009 and revised in September 2013), https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.

[205] See ENISA, "Privacy and Data Protection by Design", op. cit., "Although the [PbD] concept has found its way into legislation as the proposed European General Data Protection Regulation, its concrete implementation remains unclear at the present moment.", p. iii.

[206] Woodrow Hartzog, "Privacy's Blueprint: The Battle to Control the Design of New Technologies" (Harvard Univ. Press 2018), Part One, *The Case for Taking Design Seriously in Privacy Law,* Chapter One, *Why Design is Everything.*

> *time for privacy engineering has arrived as a necessary component to constructing systems, products, processes, and applications that involve personal information. ”*[207]

PbD is also recognized as a best practice by leading domestic and international regulatory authorities[208] when it is not enshrined as a legal obligation. For example, the EU General Data Protection Regulation (GDPR) makes PbD mandatory for data controllers and processors “both at the time of the determination of the means for processing and at the time of the processing itself”[209].

Incorporating privacy and pseudonymity (i.e., disguised identity)[210] into the product/service delivery model allows municipalities to build trust with citizens by demonstrating responsibility with sensitive data. The public’s trust in IoT technologies will be vital for the sustained evolution of Smart Cities and will rely upon the ability to securely modernize public services.[211]

Privacy is garnering a lot of additional attention in 2018 in both the European Union (e.g., above-mentioned GDPR and its *lex specialis,* i.e., the forthcoming [as of July 2018] ePrivacy Regulation[212]) and the United Sates (see pending bills in Congress[213]). Furthermore, on May 11, 2018, ISO, the International Organization for Standardization headquartered in Geneva, Switzerland, put PbD front and center in consumer IoT when it announced that:

> *“As new EU regulations come into force late this month [May 2018] that require companies to protect personal data, restricting the way it is collected and used, ISO is taking the consumer voice one step further. A team of privacy experts has been formed to develop the first set of preventative international guidelines for ensuring consumer privacy is embedded into the design of a product or service, offering protection throughout the whole life cycle. The new ISO project committee, ISO/PC 317*[214]*, Consumer protection: privacy by design for consumer goods and services, was developed by ISO/COPOLCO, the ISO committee that deals with consumer issues in standardization. Its remit is to develop a standard that will not only*

[207] Michelle Finneran Dennedy, Jonathan Fox & Thomas Finneran, “The Privacy Engineer’s Manifesto: Getting from Policy to Code to QA to Value,” Apress, January 2014, pp. 7-8.

[208] The focus on data protection and privacy is uneven around the world. See for example, Abdi Latif Dahir, May 8, 2018, “Africa isn’t ready to protect its citizens personal data even as EU champions digital privacy”, https://qz.com/author/adahirqz/

[209] See Article 25 of GDPR: ”Data protection by design and by default” https://gdpr-info.eu/art-25-gdpr/

[210] ENISA, “Privacy and Data Protection by Design”, op. cit.,: “It is important to note that long-term pseudonyms run the risk of becoming as revealing as real identities, as users perform linkable actions and leak an increasing amount of identifying or personal information over time. It is therefore good practice to allow users to refresh their pseudonyms or have control of more than one at a time.”, p. 29.

[211] Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics (Heraklion: ENISA, 2015, ©2015), 1-80, accessed July 24, 2017, https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics

[212] See https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[213] See pending privacy legislation (some of it related to IoT) in the 115th U.S. Congress as reported by the Association of National Advertisers as of April 9, 2018 here: http://www.ana.net/getfile/26427

[214] https://www.iso.org/committee/6935430.html

> *enable compliance with regulations, but generate greater consumer trust at a time when it is needed most."* [215]

Privacy is an element of paramount significance in the relationship of trust between the citizen and the city. However, other considerations must be factored in to trust an IoT undertaking. As mentioned above[216], NIST has developed a thorough trustworthiness reference model encompassing security, privacy, safety, reliability and resilience.[217] Note in passing that privacy is a recent arrival in the trustworthiness toolbox of the Internet of Things (see Figure 16 below).

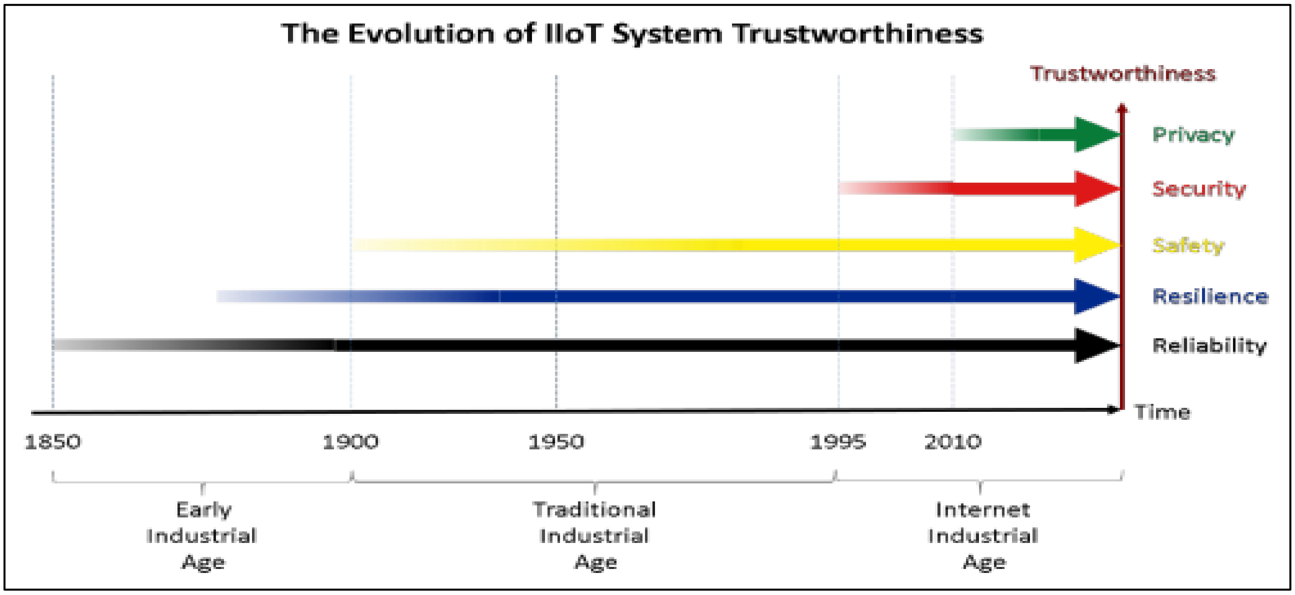


Figure 16: Industrial Internet of Things Trustworthiness[218]

In February 2018, in its "Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)" cited elsewhere in this report (e.g., section 3.2 IoT Security), NIST reiterated that "trustworthiness of IoT systems will require active management of risks for privacy, safety, security, etc." (p. 33).

[215] Clare Naden, "Data privacy by design: a new standard ensures consumer privacy at every step", May 11, 2018 https://www.iso.org/news/ref2291.html

[216] See Section 3.2 IoT Security

[217] See NIST, "Exploring the Dimensions of Trustworthiness: Challenges and Opportunities," workshop on August 30-31, 2016, videos are accessible here: https://www.nist.gov/news-events/events/2016/08/exploring-dimensions-trustworthiness-challenges-and-opportunities

[218] Source: Jesus Molina, Security Consultant, Fujitsu & Co-chair IIC Security Working Group, "The Challenge of Securing the Industrial Internet - An overview of the IIC Security Framework,", Industrial Internet Consortium Blog, June 21, 2016, http://blog.iiconsortium.org/2016/06/the-challenge-of-securing-the-industrial-internet.html

While in agreement with NIST that the above five trustworthiness properties can be "applied most broadly across the diverse breadth of Cyber-Physical [IoT] Systems"[219], additional elements, which admittedly might be somewhat more difficult to quantify or delineate, could also be included to establish a trusting environment. For example, quality, transparency, competence, user-centeredness and ethics are such components[220].

5.3 Seamless IoT Device Connection as a Critical Enabler

Billions of smart devices ("massive IoT"[221]) will be coming online in the near future, making connection especially challenging. Technical and non-technical factors, which depend on both the applications and the specific Smart City itself, come into play.

From an engineering viewpoint, IoT introduces new constraints that weigh on the design of a seamless connection network. Some technical factors include, but are not limited to:

- Bandwidth
  - This includes both per device and aggregate bandwidth needs.
- Coverage
  - Is the area to be covered large or localized?
- Power requirements of devices

[219] NIST, Framework for Cyber-Physical Systems, Release 1.0, op. cit., pp. 80-81.

[220] For conceptual purposes, see the following (theoretical) multiplicative model (i.e., if any dimension fails [= 0], the IoT project under consideration, whatever it is, is not trusted [Trust = 0]):

$T = \alpha SE^{a} \cdot \beta PR^{b} \cdot \gamma SA^{c} \cdot \delta RL^{d} \cdot \varepsilon RS^{e} \cdot \zeta QY^{f} \cdot \eta TR^{g} \cdot \theta CO^{h} \cdot \iota UC^{i} \cdot \kappa ET^{j} \cdot \text{Error Term}$

Endogenous Variable (explained by the model):
T = Trust (overall trust in IoT solution(s)/system/architecture)

Exogenous (explanatory) Variables (if any = 0 then trust = 0):
SE = Security (confidentiality, integrity, availability, etc.)
PR = Privacy (protection of personal information)
SA = Safety (absence of catastrophic consequences on life, health, property, or data of stakeholders)
RL = Reliability (availability, dependability, predictability, maintainability, consistency)
RS = Resilience (plasticity, i.e., swift recovery from disruptions)
QY = Quality (conformance to requirements, fit to purpose)
TR = Transparency (complete openness on processes, data storage, and use)
CO = Competence (provider's technical and operational knowledge and expertise)
UC = User-Centeredness (user friendliness, ease of access, user experience focus)
ET = Ethics (throughout the building and delivery of the product, e.g., honesty, equity, etc.)
Error = Other elements (combined effect of omitted variables determining trust)
Coefficients:
$\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta, \iota, \kappa$ = Relative weight of each variable
a, b, c, d, e, f, g, h, i, j = respective partial elasticities (>0)
Source: CDAIT internal notes and discussions.

[221] 5G Americas, "LTE Progress Leading to the 5G Massive Internet of Things", December 2017, op. cit.

    - If devices must operate for a long time on a single charge, the distance they need to transmit may have to be minimized.
- Density of “things”
    - How many devices will be deployed per square mile?
- Total number of devices
    - This can impact bandwidth and media access designs.
- Frequency of network access per device
    - Occasional transmission of an action (e.g. a parking gate opening/closing) has different needs than constant transmission of video data.
- Security
    - This includes both cybersecurity and physical security of the device.
- Time Proofing
    - Integration with legacy equipment/systems[222] (past proofing) and protection against premature obsolescence (future proofing).
- Standards
    - Necessary to permit interoperability,

While these answers lie with the engineers and network architects, non-technical factors also affect the operations of the Smart City and the vendors that support it. Some of these factors, beyond privacy and ethical considerations addressed elsewhere in this White Paper, include:

- Ownership of the devices
    - Will the vast array of devices be owned by the city, owned by a central third party that leases access to the city, or owned by disparate multiple entities (e.g., businesses, citizens, government, etc.) with sharing agreements? There are multiple models for how device ownership can be managed.
- Ownership of network connectivity

[222] As an example of dealing with legacy, Georgia Tech researchers Arshdeep Bahga, Vijay K. Madisetti, Raj K. Madisetti, and Andrew Dugenske (2016) in “Software Defined Things in Manufacturing Networks”, Journal of Software Engineering and Applications, 9, 425-438 proposed “a Software-Defined Industrial Internet of Things (SD-IIoT) platform for as a key enabler for cloud-manufacturing, allowing flexible integration of legacy shop floor equipment into the platform,” http://www.scirp.org/journal/PaperInformation.aspx?PaperID=70433&#abstract. The Georgia Tech Manufacturing Institute (GTMI)’s Centers and Laboratories are listed here: http://www.manufacturing.gatech.edu/centers-labs

  - There may be one central network or (more likely) multiple networks supporting the competing needs of the IoT devices. Will the Smart City, businesses, and other organizations deploy and own their own network(s)? Will they lease the network infrastructure itself from a third party? Will they lease network access from a third party (similar to today's mobile phone model)? These decisions influence future budgeting, staffing, and usability planning for all parties involved.

- Ownership of data
  - As data is collected, who is responsible for its curation, access control, anonymization, distribution, and archiving?
- Financial ownership and accountability: Who pays for what and how?
  - A recent Deloitte White Paper emphasizes that any broad-based Smart City reinvestment and modernization program "forces city governments to carefully consider the cost benefit of pursuing a particular project or suite of projects, as well as new models for funding and financing infrastructure programs." [223]

When considering the use of IoT technologies for Smart Cities, all of these dimensions should be integral to a comprehensive approach.

Too often IoT technologies are implemented in a piecemeal fashion, solving narrowly defined problems. It follows that multiple IoT device configurations, each intended to address a targeted situation, end up being a juxtaposition of capabilities without synergistic and strategic efficiencies. However, over time, they organically morph into an overall architecture, calling for policies and procedures to enable it to function optimally moving forward.

In order to avoid this type of disjointed effort, cooperation of all stakeholders is required from the beginning to ensure unified and productive operations (see 5.5 Integration below).

5.4 USE CASES

5.4.1 Municipal Services Management

Launched in June 2014, the Uraía Platform was established as a collaboration between two international institutions working to improve the life of urban citizen's around the world: Global Fund for Cities Development (FMDV) and the Local government and decentralization Unit of UN-Habitat. Both institutions believe that SMART technologies

[223] Steve Hamilton and Ximon Zhu, Deloitte Center for Government Insights, 2017, "Funding and Financing Smart Cities", https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-ps-funding-and-financing-smart-cities.pdf . See also Clyde Wayne Crews, Jr., "Who will own the infrastructure in the Smart City?", January 11, 2018, Forbes, https://www.forbes.com/sites/waynecrews/2018/01/11/who-will-own-the-infrastructure-in-the-smart-city/#7afb94781ab4

represent an extraordinary opportunity to reinforce the capacity of local governments to respond to the accelerated urban challenges and the increasing citizen´s demands.

On April 19 and 20th, 2016, Uraía held a workshop in Nicosia, Cyprus to exchange experiences on initiatives that used SMART technologies to improve tax recovery and increase energy efficiency and how these experiences produce an impact on municipal budget and are transformed into better services to all citizens.

The following statement spells out how the opportunity created by digital (including IoT) technologies spans from productivity improvement to efficient service delivery reflecting user demands.

> *"Local governments around the world have been using ICT to improve management efficiency and service delivery to citizens and businesses for decades. The rapid evolution of ICT with the advent of SMART technologies (smartphones, Internet of Things, big data, analytics, SMART cloud, etc.) have provided renewed opportunities for the optimization of municipal management. Not only technology has changed but also the approach that local governments have towards it, evolving from digitization, to e-government and, more recently, towards digital governments. While the first two aimed mainly at improving productivity in administrative services, the digital government approach is more focused on the use of SMART technologies to reflect the user demands. The digital government employs innovative changes in service design, management and delivery; providing greater openness, transparency, engagement and interaction between the citizen and the administration and between services within the municipality."*[224]

Their recommendations for the future, which can be construed as a sound roadmap for the insertion of smart technologies in the creation and delivery of municipal services, are presented below:

Preparation

1. To choose the technology and projects according to the city's vision;
2. To choose the technology according to the municipality's capacities;
3. To strengthen institutional capacities and invest in skilled human resources;
4. To provide political leadership;
5. To start with pilot projects in small areas;
6. To define a clear and flexible legal and regulatory framework;
7. To ensure data privacy and cybersecurity;
8. To carry out the necessary studies, and particularly when the municipality is considering to implement SMART projects in partnership with the private sector;
9. To ensure systems interoperability and avoid isolated initiatives.

[224] Uraia, "The Impact of SMART Technologies in the Municipal Budget: Increased Revenue and Reduced Expenses for Better Services," report produced in December 2016, http://www.uraia.org/files.uploads/nicosia-guidelines-uraia-2016-eng

Collaboration

10. To cooperate with national government and association of cities;
11. To ensure dialogue and coordination with multiple stakeholders;
12. To guarantee integration between city departments.

Encouraging Use

13. To conduct strong on-going communication and sensitization campaigns;
14. To establish incentives;
15. To combine traditional and online solutions.

No roadmap to successfully guide cities into the future can overlook sustainability, increasingly becoming a key component of urban planning – see for example the 2018 assessment from the United Nations Environment Programme's International Resource Panel on the "Weight of Cities."[225]

In many cases, IoT is being viewed as a sustainability enabler if not a potential "game changer":

> *"Most current IoT projects can contribute to achieving both the SDGs [United Nations' Sustainable Development Goals] and the UN's 2030 mission. An analysis of more than 640 IoT deployments, conducted in collaboration with IoT research firm IoT Analytics, showed that 84% of existing IoT deployments can address the SDGs."*[226]

[225] See Working Group on Cities of the International Resource Panel (IRP) (2018), "The Weight of Cities: Resource Requirements of Future Urbanization," Swilling, M., Hajer, M., Baynes, T., Bergesen, J., Labbé, F., Musango, J.K., Ramaswami, A., Robinson, B., Salat, S., Suh, S., Currie, P., Fang, A., Hanson, A. Kruit, K., Reiner, M., Smit, S., Tabory, S. A Report by the International Resource Panel. United Nations Environment Programme, Nairobi, Kenya.http://www.resourcepanel.org/file/971/download?token=ehOygAQ7. Although the report acknowledges that 'smart' technologies (including IoT technologies) can be used to improve resource efficiencies, it submits that a smart city is not synonymous with a sustainable city and argues for shifting the paradigm to "well-grounded cities". Another concept that goes beyond "smart city", addressing sustainability and more is "resilient city", see "100 Resilient Cities" website: http://www.100resilientcities.org/about-us/ . Note the key role of IoT technologies for resilient cities as well – see Ken Dodson, "Urban Resilience: Engaging your Community through Data," Cisco Blog, March 5, 2018 https://blogs.cisco.com/government/first-steps-to-resilient-cities-community-engagement-and-kinetic

[226] IoT as a "game-changer" for sustainability is advanced by Rodrigo Arias in "The effect of the Internet of Things on sustainability," World Economic Forum, January 21, 2018 https://www.weforum.org/agenda/2018/01/effect-technology-sustainability-sdgs-internet-things-iot/. As far as IoT technologies as sustainability enablers see ITU IoT Week's "Internet of Things Declaration to Achieve the Sustainable Development Goals," (June 6-9, 2017, Geneva, Switzerland): http://iot-week.eu/wp-content/uploads/2017/06/IoT4SDG-Declaration.pdf; and World Economic Forum's "Future of Digital Economy and Society System Initiative: Internet of Things Guidelines for Sustainability," (January 2018): http://www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf.

Colleges and universities around the world are embracing sustainability through applying sustainable practices to their own operations and exploring the scientific, technological, business and policy aspects of sustainability including within a city framework[227].

5.4.2 Utilities: Smart Electric Grid

TOKYO, JAPAN

In 2017, Tokyo Electric Power Company (TEPCO) reached a milestone of 10 million advanced meters and devices to become the world's largest Internet of Things (IoT) utility network.[228]

> *"Currently, the network is moving data between devices at a rate of 513 million interval reads per day which will climb to 1.3 billion interval data packets daily."*

Within seven years, TEPCO said it would have 30 million utility and consumer devices operating on the network.

> *"Tokyo comprises an entire suburban area known as a "smart town", which produces zero carbon emissions and is entirely powered by renewable energy /…/ The Japanese division of the Global Carbon Project, which is dedicated to meeting the world's carbon challenges, is working on a Tokyo smart city project in collaboration with a host of government bodies and universities."*[229]

Achieving energy efficiency through smart meters in an urban environment is an important step towards managing climate change:

> *"Cities are major contributors to climate change: although they cover less than 2 per cent of the earth's surface, cities consume 78 per cent of the world's energy and produce more than 60% of all carbon dioxide and significant amounts of other greenhouse gas emissions, mainly through energy generation, vehicles, industry, and biomass use."*[230]

[227] See the Association for the Advancement of Sustainability in Higher Education (ASHE) (created in 2006) https://www.aashe.org/; the Higher Education Sustainability Initiative (HESI) (created in 2012) https://sustainabledevelopment.un.org/sdinaction/hesi; and the following article by David Chandler, "Education leaders gather to chart a future for sustainability at universities - International meeting examines progress on campuses, explores goals for coming years," MIT News Office, September 22, 2016 https://news.mit.edu/2016/education-leaders-sustainability-universities-0922. Georgia Tech is no exception, see Rachael Pocklington, "What Does Sustainability Mean to Georgia Tech," http://www.news.gatech.edu/features/what-does-sustainability-mean-georgia-tech

[228] SmartCitiesWorld NewsTeam, "World's largest intelligent grid deployment milestone," April 28, 2017 http://smartcitiesworld.net/news/news/worlds-largest-intelligent-grid-deployment-milestone-1627

[229] See Felix Todd, "Smartest cities in the world – which places are ahead of the game in connectivity?" Compello, July 4, 2018 https://www.compelo.com/smartest-cities/. Note that, as related in the article, Georgia Tech under the leadership of Dr. Perry Yang, Associate Professor, School of City & Regional Planning and School of Architecture, and Director (US side) of the Sino-U.S. Eco Urban Lab http://www.ecourbanlab.org/ contributes to the Tokyo Smart City project, see https://design.gatech.edu/news/georgia-tech-kicks-tokyo-smart-city-studio-project-2020-olympic-site-0

[230] United Nations – Habitat for a Better Urban Future website, https://unhabitat.org/urban-themes/climate-change/

5.4.3 Public Safety

According to a June 2018 press release from Market Research Future on public safety for Smart City (see Figure 17 as well):

> *"The public safety solution for smart city market is growing because of the growing adoption of internet of things. Some of the factors driving the growth of the market is that residents want to live in clean and safe environment, entrepreneurs aspire to create innovative solutions and economic opportunity, residents and visitors like to get around town easily, smart cities enhance quality of life, making them great places to live. Due to high adoption of cloud and internet of things, the public safety solution for smart city market is growing explosively. The adoption of public safety solution for smart city market is used mostly in public transportation security, critical infrastructure security, disaster management, medical emergency service, firefighting services, law enforcement and intelligence agencies. The advantages of public safety solutions for smart city market are to exceed public expectations, maximize public budgets, manage complex systems and reduce response times."*

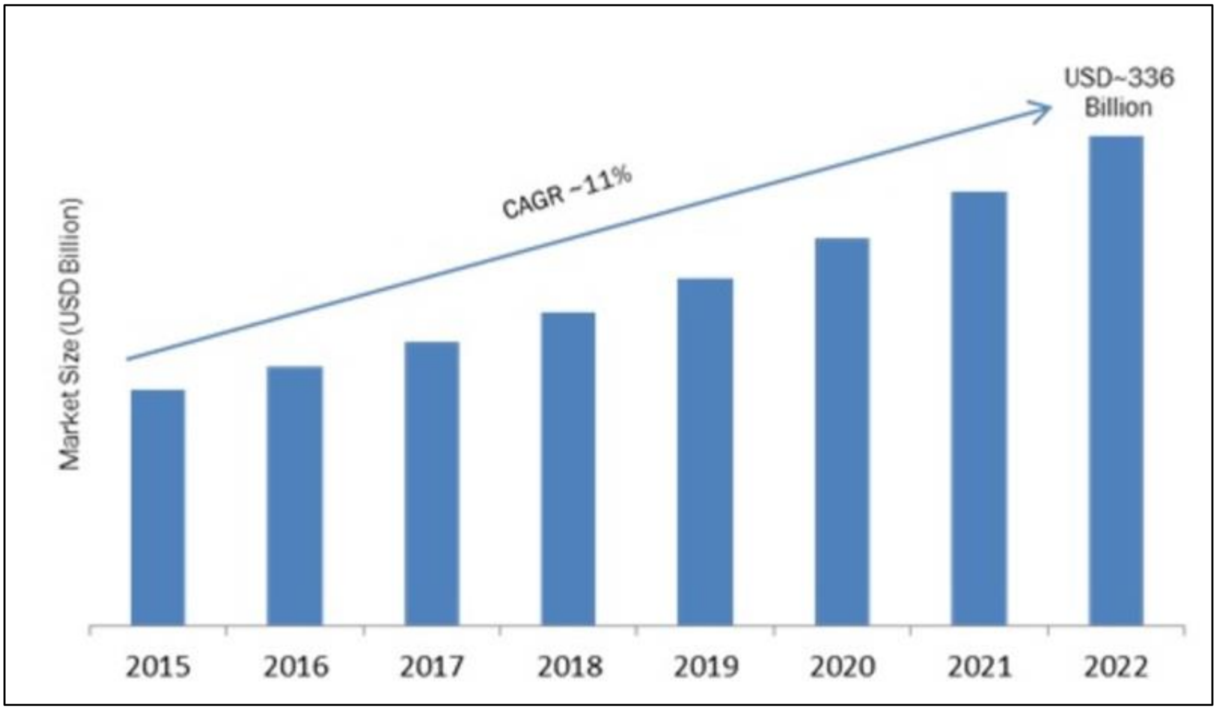


Figure 17: Public Safety Solution for Smart City Market[231]

[231] Source: Market Research Future Press Release, "Public Safety Solution For Smart City Market Research Report- Global Forecast to 2022," June 2018 https://www.marketresearchfuture.com/reports/public-safety-solution-smart-city-market-2738

5.4.4 Transportation

Growing urban populations steadily increase traffic congestion. Density variations can decrease vehicle speeds at peak and non-peak commuting times. The future infrastructures must be able to manage real time traffic density using IoT. This can optimize traffic light switching and real-time status availability to smart devices, and provide alternative paths to avoid traffic jams.[232]

SÃO PAULO, BRAZIL

A diagnostic exercise conducted in 2014 confirmed that road safety management in São Paulo lacked coordination. Agencies that were focused on this lacked synergy and comprehensive performance management data. In early 2015 a government decree established a working group to draw up the Movimento Paulista de Segurança no Trânsito (MPST) road safety project, a partnership between the State of São Paulo and the non-governmental organization, Centro de Lideranca Publica.

The resulting engagement of government agencies, private sector partners, and consultants led to the creation of a state action plan for road safety and the MPST project, which in its first year comprised:

- The building of a data system (INFOSIGA SP) which provides monthly reports on traffic deaths in the State of São Paulo (detailing crash occurrences, contributing risk factors, crash scene descriptions, road sections, etc.) and a related mapping system (INFOMAPA SP);
- Road safety actions in 15 cities were focused on three main areas: road infrastructure (traffic lights, crosswalks, pedestrian barriers, elevated crosswalks and sidewalks); traffic education (traditional and social media awareness campaigns, simulated traffic accident victims rescue); and traffic supervision (traffic blitz, repositioning of transit agents);
- A governance structure to monitor results with a high-level Management Committee (representing State Secretariats) and Executive Committee (representing participating road agencies).

In the first year of the MPST project, an estimated 71 lives were saved in the 15 participating cities, compared with the previous year, a reduction of 14.3% (compared with a 5.8% reduction across the state of Sao Paulo). Adjusting this to reflect an incremental

[232] See the following article about the Atlanta North Avenue Smart Corridor, which will “serve as a public demonstration and “living lab” for Internet of Things (IoT) deployment, data collection and analytics, connected and autonomous vehicles, and unique partnerships to fundamentally transform how Atlanta plans for, designs and operates its transportation infrastructure,” .Ben Levine, “Atlanta's Smart Corridor to serve as "Living Lab" for Smart Transportation,” Government Technology, October 13, 2017. http://www.govtech.com/civic/Atlantas-Smart-Corridor-to-Serve-as-Living-Lab-for-Smart-Transportation.html

improvement over and above the state improvement suggests a gain of 42 lives saved as a result and an estimated 420 serious injuries avoided.[233]

ATLANTA, GA, U.S.A.

With the goal of creating safer roads for drivers, over 100 variables were combined in order to determine root cause of crashes and forecast warning alerts. Project objectives include:

1. Data Aggregation and Visibility – Summarize collision findings from multiple data sources
2. Root Cause Identification – Determine the root causes that impact collision risk levels
3. Forecast Risk Indices/Warning Alerts – Develop models that predict risk levels for collisions[234]

Relevant themes include traffic constraints and collision risks as well as North Avenue-specific observations.

- Average number of collisions per week in Atlanta have increased by about 30% since 2012 with wide variations observed from week to week
- Incidence of automobile collisions are typically lowest around the seasonal holidays (Nov.-Dec.)
- The most frequent collisions occur on city streets, but the most severe ones occur on highways
- Specific attributes of weather can have a distinct impact on number and severity of collisions

LOS ANGELES, CA, U.S.A.

Evolving smart and adaptive street lights are making a difference in the nation's second largest city. A key Smart City/Community sensor solution is streetlight control and management. Streetlights offer a power source via standard receptacles and an ideally located infrastructure for sensor mounting. In time, officials also will have the ability to brighten, dim, blink the lights and gather environmental information on an area.

Los Angeles has about 50,000 smart street lights operating around the city. The city plans to upgrade the remaining 110,000 lights with remote monitoring units and smart controls over the next few years. CNN Money reported that the City of Los Angeles has saved $8 million a year thanks to the new LED bulbs, cutting energy use by 60 percent. Without

[233] See Together for Safer Roads website, São Paulo, http://www.togetherforsaferroads.org/sao-paulo-brazil/

[234] Miro Holecy, Global Solutions Leader and CTO, Intelligent Transportation - IBM, Success Stories Using Data, Drive Sweden, May 31, 2017, slide 5, https://www.drivesweden.net/sites/default/files/content/ibm_reference_cases.pdf

having to rely on reports from residents, the City can replace lights that have burned out at a faster rate, providing safety and quality-of-life benefits as well.[235]

PARIS, FRANCE

It is estimated that the average Parisian spends nearly four years in their lifetime searching for parking. Paris is focused on changing that. The city's new digital platform enables organizations to leverage citywide parking data to develop apps and tools that can alert drivers of available parking spaces in the area, allow for the booking of spaces in advance, and enable secure remote payment options. These applications attempt to minimize time, physical energy and fuel costs for combing the streets looking for a parking space.

Paris is also attempting to maintain cleanliness and support public waste management services by efficiently using public trash bins. Cities and communities can leverage sensor technology to inform when and where public trash bins reach capacity, allowing city officials to redirect collection services on an as-needed basis. This 'smart bin' method saves time by avoiding unnecessary pickups for empty or barely full bins, conserves truck fuel, and enhances employee productivity.[236]

SAN FRANCISCO, CA, U.S.A.

To determine the appropriate price to charge for parking to meet parking-space availability targets, SFpark, an innovative project of the San Francisco Municipal Transportation Authority, uses wireless sensors to detect occupancy in metered spaces. Installed in 8,200 on-street spaces in the pilot areas, the wireless sensors detected parking availability in real time. Sensors also were placed in three control neighborhoods to provide baseline data for evaluation purposes.

In 2013, two years after launching SFpark, San Francisco announced that the program had reduced weekday greenhouse gas emissions by 25 percent. Traffic volume shrank, and drivers cut their parking search time nearly in half.

They achieved these results by adjusting pricing to incentivize drivers to do things such as park in less congested areas, or arrive and leave at off-peak times.

San Francisco increased revenues by about $1.9 million by making it easier to pay for their parking. Before SFpark, only 45 percent of drivers fed the meter during the workweek. During the pilot, that number rose to 54 percent. The difference was enough to offset the revenue lost to decreased parking tickets.[237]

[235] Kate Meis, "3 ways IoT is already making cities smarte,", Green Biz, June 1, 2016 https://www.greenbiz.com/article/3-ways-iot-already-making-cities-smarter

[236] Harold Bell, "Digital Impact to Public Works and Utilities," Cisco blog, November 21, 2016 https://blogs.cisco.com/government/digal-impact-to-public-works-utilities

[237] Kate Meis op. cit.

SHANGHAI, CHINA

In early 2017 TSR ("Together for Safer Roads") announced that:

> *"Working with the Tongji University Joint International Research Laboratory of Transportation Safety, TSR (Together for Safety Roads) is supporting the establishment of a collaborative mechanism between government, business, academia, and non-governmental organizations to enhance the safety of Shanghai's transportation. This collaboration is aligned with Shanghai's Transportation goal to reduce the road fatality rate from 3.73 to 2.63 fatalities per 100,000 motor vehicles by 2020. TSR is providing its skills and subject matter expertise to support three programs: 1) crash hotspot analysis and improvement; 2) behavior-based commercial driver safety analysis education; and 3) safer users through road safety awareness campaigns."*[238]

5.4.5 Healthcare

According to a 2018 Deloitte White Paper on the *Global Health Care Outlook – The Evolution of Smart Health Care*[239]

> *"Development of the IoT in the health care market (where it is also called the Internet of Medical Things, or IoMT) has been proving particularly valuable in remote clinical monitoring, chronic disease management, preventive care, assisted living for the elderly, and fitness monitoring. IoT's application is lowering costs, improving efficiency, and bringing the focus back to quality patient care."*

A 2018 Intel-sponsored study by Juniper Research[240] confirmed these findings in a smart city context:

> *"Smart cities with connected digital health services can play a significant role in creating efficiencies – saving citizens almost 10 hours a year – and even potential lifesaving benefits for both patients and caregivers. Examples such as wearable apps monitor blood pressure, pain tolerance and temperature to help people manage chronic conditions without hospitalization. "Telemedicine" enables contagious flu sufferers to avoid doctor's offices with an examination via high-speed video link from the comfort of their home."*[241]

[238] TSR press release, "Together for Safer Roads Partners with Three Global Cities to Address Critical Road Safety Challenges," February 21, 2017, http://www.togetherforsaferroads.org/press/press-release-safer-roads-challenge/

[239] Deloitte, "2018 Global Health Care Outlook – The Evolution of Smart Health Care," p.17 https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/life-sciences-health-care/deloitte-cn-lshc-2018-global-health-care-sector-outlook-en-180322.pdf

240 Intel Newsroom, "Smart Cities Technologies Give Back 125 Hours to Citizens Every Year," Intel website, March 12, 2018, https://newsroom.intel.com/news/smart-cities-iot-research-125-hours/

241 An example of IoT technologies aiming to improve the management of chronic diseases can be found here: Qualcomm press release, "Qualcomm and Boehringer Ingelheim Pharmaceuticals collaborate to add

The above Deloitte White Paper complements an earlier article on IoT in healthcare[242] and a previous White Paper on the Hospital of the Future[243], which gives a useful roadmap for the insertion of digital (including IoT) technologies in hospitals (see below):

> *"• **Redefined care delivery**: Emerging features including centralized digital centers to enable decision-making, continuous clinical monitoring, targeted treatments (such as 3-D printing for surgeries), and the use of smaller, portable devices will help characterize acute care hospitals.*
>
> *• **Digital patient experience**: Digital and artificial intelligence (AI) technologies can help enable on-demand interaction and seamless processes through a choice of devices to improve patient experience.*
>
> *• **Enhanced talent development**: Robotic process automation (RPA) and AI can allow caregivers to spend more time providing care and less time documenting it; as well as help enhance development and learning among caregivers.*
>
> *• **Operational efficiencies through technology**: Digital supply chains, automation, robotics, and next-generation interoperability can drive operations management and back-office efficiencies.*
>
> *• **Healing and well-being designs**: The well-being of patients and staff members—with an emphasis on the importance of environment and experience in healing—will likely be important in future hospital designs.*
>
> *Technology will likely underlie most aspects of future hospital care, but care delivery—especially for complex patients and procedures—may still require hands-on human expertise. Many future technologies can supplement and extend human interaction."*

new digital technology to RESPIMAT® inhaler," Qualcomm newsroom, August 30, 2016 https://www.qualcomm.com/news/releases/2016/08/30/qualcomm-and-boehringer-ingelheim-pharmaceuticals-collaborate-add-new

[242] Luc Brucher and Safaa Moujahid,"A revolutionary digital tool for the healthcare industry: The Internet-of-Things," Inside Magazine – Issue 15, Deloitte, June 2017, https://www2.deloitte.com/tr/en/pages/life-sciences and-healthcare/articles/digital-health-iot.html

[243] Deloitte, "The hospital of the future: How digital technologies will change hospitals Globally,", Deloitte Center for Health Solutions, 2017, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/us-lshc-hospital-of-the-future.pdf

5.5 Integration

Many factors should be considered when designing and implementing smart city initiatives; from security to connectivity, not only within the underlying city infrastructure, but within the community as well. A bird's-eye view is necessary to embrace the complexity, interconnectedness, and interplay inherent to Smart Cities.

The community is the ultimate benefactor. TM Forum's *City as a Platform Manifesto* (see Table 9 below) reflects this focus.

1.	City platforms must enable services that improve the quality of life in cities; benefiting residents, the environment, and helping to bridge the digital divide.
2.	City platforms must bring together both public and private stakeholders in digital ecosystems.
3.	City platforms must support sharing economy principles and the circular economy agenda.
4.	City platforms must provide ways for local start-ups and businesses to innovate and thrive.
5.	City platforms must enforce the privacy and security of confidential data.
6.	City platforms must inform political decisions and offer mechanisms for residents to make their voices heard.
7.	City platforms must involve the local government in their governance and curation, and be built and managed by the most competent and merited organizations.
8.	City platforms must be based on open standards, industry best practices and open APIs to facilitate a vendor neutral approach, with industry agreed architecture models.
9.	City platforms must support a common approach to federation of data or services between cities, making it possible for cities of all sizes to take part in the growing data economy
10.	City platforms must support the principles of the UN Sustainable Development Goal 11 – "Making cities and human settlements inclusive, safe, resilient and sustainable."

Table 9: City as a Platform Manifesto[244]

[244] Arti Mehta, "City as a Platform Manifesto: Ten common principles driving smart city success," September 20, 2017 https://inform.tmforum.org/internet-of-everything/2017/09/city-platform-manifesto-ten-common-principles-driving-smart-city-success/

A critical question at the heart of the Smart City development is what kind of priority to give to each need category. The same way Abraham Maslow identified a hierarchy of human needs[245], some have argued that there is a logical progression that must be satisfied in meeting the needs of the city and its citizens; for instance, physiological and safety needs should be met before considering addressing higher level objectives. – see Figures 18 and 19 below:

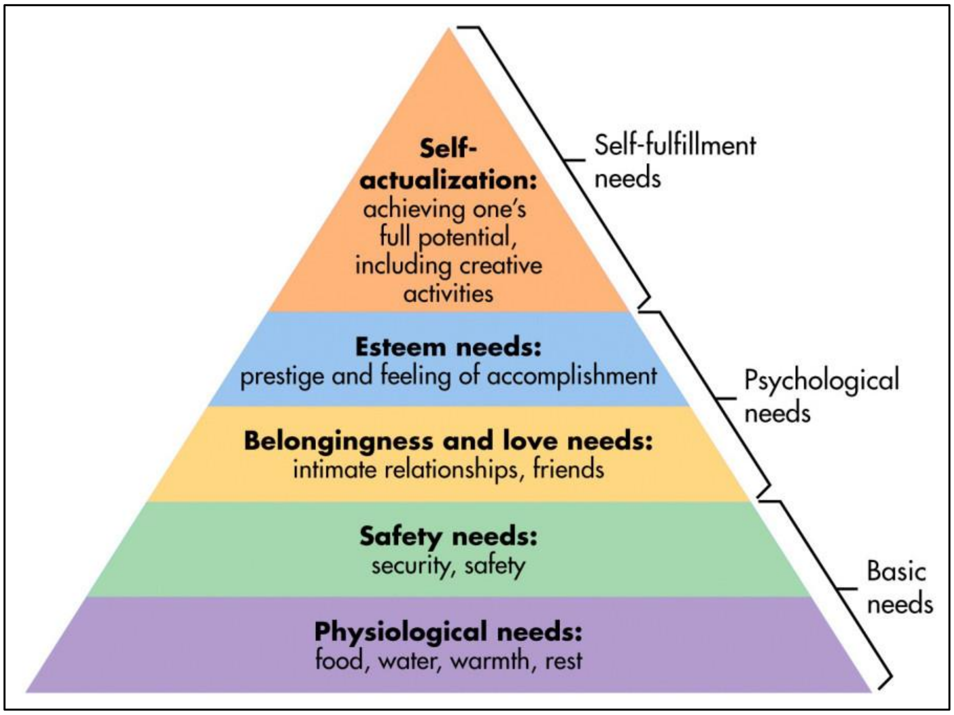

Self-actualization: achieving one's full potential, including creative activities
Esteem needs: prestige and feeling of accomplishment
Belongingness and love needs: intimate relationships, friends
Safety needs: security, safety
Physiological needs: food, water, warmth, rest
Self-fulfillment needs
Psychological needs
Basic needs

Figure 18: Maslow's Hierarchy of Needs[246]

[245] Maslow, A. H. "Theory of Human Motivation", *Psychological Review*, 1943, *50*, 370-396, http://psychclassics.yorku.ca/Maslow/motivation.htm. See also: Stephen DeAngelis, "Towards a Smart City Hierarchy of Needs", October 12, 2016, https://www.linkedin.com/pulse/towards-smart-city-hierarchy-needs-stephen-deangelis, and this interesting take on Maslow's Hierarchy of Needs and Digital Citizens: José Luis Carrasco-Sáez, Marcelo Careaga Butter, and María Graciela Badilla-Quintana, "The New Pyramid of Needs for the Digital Citizen: A Transition towards Smart Human Cities", December 2017, MDPI, www.mdpi.com/2071-1050/9/12/2258/pdf

[246] Saul McLeod, "Maslow's Hierarchy of Needs," SimplyPsychology, May 21, 2018, https://www.simplypsychology.org/maslow.html; pdf version (2017): https://www.simplypsychology.org/simplypsychology.org-Maslows%20Hierarchy%20of%20Needs.pdf

;

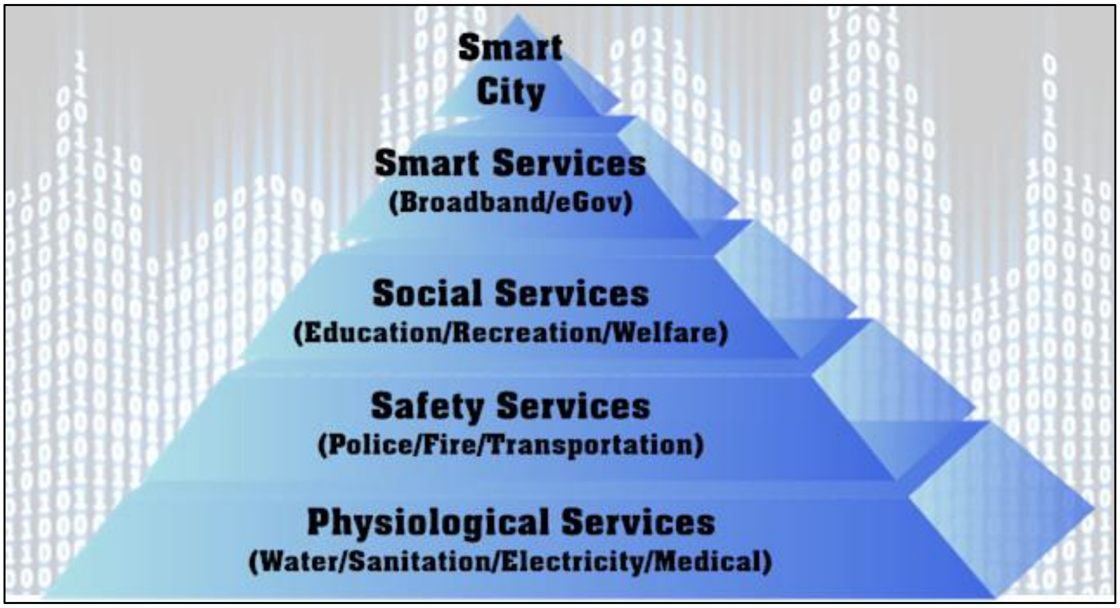

Smart City
Smart Services
(Broadband/eGov)
Social Services
(Education/Recreation/Welfare)
Safety Services
(Police/Fire/Transportation)
Physiological Services
(Water/Sanitation/Electricity/Medical)

Figure 19: Smart City Hierarchy of Needs[247]

Innovations such as online meters to manage water infrastructure remotely, maximize workforce and minimize waste of resources[248]; smart lighting to decrease power consumption[249]; and parking applications to find open spots[250] are but a few examples that illustrate how cities have developed original solutions to save time and money for the benefit of the community[251].

Looking forward, however, how will cities be able to determine systematically that the project under consideration will have maximum impact?

[247] Stephen DeAngelis, "Towards a Smart City Hierarchy of Needs," Enterra Solutions, March 22, 2016 https://www.enterrasolutions.com/blog/towards-a-smart-city-hierarchy-of-needs/

[248] See Comcast Press Release, "Comcast's MachineQ and Neptune Collaborate To Accelerate Smart City Efforts," June 12, 2018 https://corporate.comcast.com/press/releases/comcasts-machineq-and-neptune-collaborate-on-iot-solution-designed-to-accelerate-smart-city-efforts

[249] See Eaton Press Release, "Eaton and CIMCON to Showcase Smart City Solutions at the IES Street and Area Lighting Conference," September 19, 2016 http://www.eaton.com/Eaton/OurCompany/NewsEvents/NewsReleases/PCT_2837407

[250] Amanda C. Coyne, "Reserve your Mall of Georgia parking spot through new app," AJC, June 14, 2018 https://www.ajc.com/news/local/reserve-your-mall-georgia-parking-spot-through-new-app/n1Cc5DXd8SjJLG68qk3GCN/ and Becca J.G. Godwin, :You can now pay money to reserve parking spaces at Lenox Square Mall," AJC, November 10, 2017 https://www.ajc.com/news/local/parking-spots-are-reservable-lenox-square-this-holiday-season/SpVbbwYK36aMivLF93pwZM/

[251] Laura Adler, How Smart City Barcelona Brought the Internet of Things to Life," Data-Smart City Solutions, Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, February 18, 2016 http://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789;

Design thinking[252] is one approach to gathering the right of information for creating IoT solutions with optimum community benefit. It incorporates many decades' worth of research across multiple disciplines to create a path to problem solving that puts the end user (viz. the citizen) at the center of the work.

Through careful questioning, rapid prototyping and iteration, the end user can quickly provide feedback that helps assess whether a solution actually solves the need in the way he/she finds beneficial. If it does not, implementation will fail.

The Internet of Things is in its infancy and, therefore, all related activities require prudent and judicious management. If hastily deployed enabling technologies do not deliver on the expected outcomes, on both technological and human axes, cities will not be as enthusiastic in their support. As a result, if not denied, IoT innovation will be delayed.

Leveraging *Design Thinking* can at least help mitigate some of this risk. Good design affects not only the 'goodness of fit' of an IoT service to the community but also the service rollout itself.

Just like determining the most appropriate and risk-mitigated IoT monetization strategy as detailed in Question #3 (IoT Business Models), sponsors and implementers would be well served to avoid single monolithic architectures and big bang implementations and instead seek to deploy self-funding incremental releases that afford a desired and measurable outcome.

[252] Jo Szczepanska, "Design thinking origin story plus some of the people who made it all happen," Medium, January 3, 2017 https://medium.com/@szczpanks/design-thinking-where-it-came-from-and-the-type-of-people-who-made-it-all-happen-dc3a05411e53

Consider an IoT ‘results-driven release’ template stating (1) an operational target (e.g., “We intend to decrease the operational expense for public works by X %”). Add to it (2) a list of IoT functionalities to be implemented (e.g., ”By inserting smart sensors in city waste bins, communicating waste bin weight to a cell phone application designed for city waste management personnel, etc.”). Include (3) a list of complementary changes to procedures, measures, and structure (e.g., “For city district Y, department members will remove waste from container-locations defined in the sequence determined by the application”). Lastly, (4) assign metrics for scheduled measurement of the results (e.g.,”Count the number of full time equivalent (FTE) hours per week spent to make a daily run per the number of waste bins emptied”).[253]

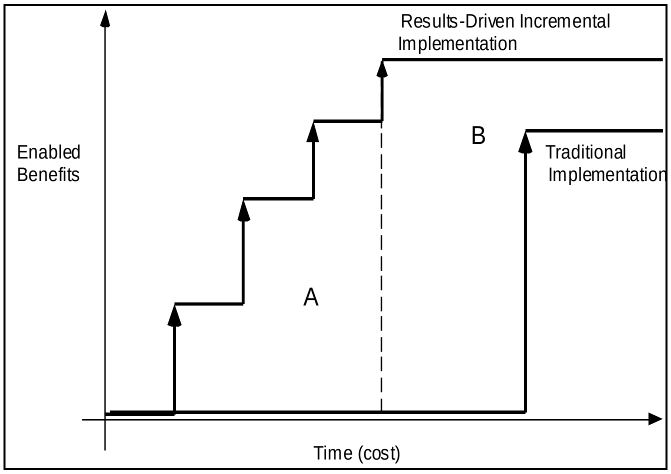


Figure 20: Results Driven Incrementalism vs. Traditional “Big Bang” Implementation[254]

The results-driven approach affords focus: Because implementers define a tight scope and scaled-down breadth of data, functionality and process changes, they only need to be responsible for a single stated and measured goal. This allows everyone to understand – in an abbreviated period of time – the benefits and shortcomings of their method and use

> *“The most obvious advantage of the RDI [Results Driven Incrementalism] approach —one shared by incremental approaches in general — is simply that the stream of business gains is realized much sooner (see area A in Figure [20]). However, implementers following the RDI approach report that it not only speeds the achievement of some benefit, but dramatically shortens the time to complete the entire initial implementation and increases the overall level of project benefits. These additional benefits (see area B in Figure [20]) arise from combining incrementalism with a strong focus on business results — a combination that has startlingly positive effects on organizational learning and implementation momentum.”*[254]

[253] Adapted from Robert G. Fichman and Scott A. Moses, “An Incremental Process for Software Implementation,” Sloan Management Review, Vol. 40, No. 2, January 15, 1999 pp. 39-52 https://sloanreview.mit.edu/article/an-incremental-process-for-software-implementation/

[254] Source: Fichman and Moses, op. cit.

this for learning and refinement as the IoT service scales up and out to other districts or municipalities.

Second, creating a series of “results-driven releases” affords more operational and financial benefits in structurally less time than a multi-function, all districts at once approach (see Figure 20 above). The approach can be marketed as a self-funding solution roadmap.

Self-funding approaches also allow cities to free up money to invest in other areas or to maintain spending at a reasonable level (see above discussion on funding and financing in section 5.3 Seamless IoT Device Connection – Financial ownership and accountability).

As cities consider where to go next, they have a real opportunity to incorporate a citizen-centric view into their plans. Using a *Design Thinking* approach for the next wave of investment can identify solutions with true citizen value that can help create the tipping point for mass adoption.

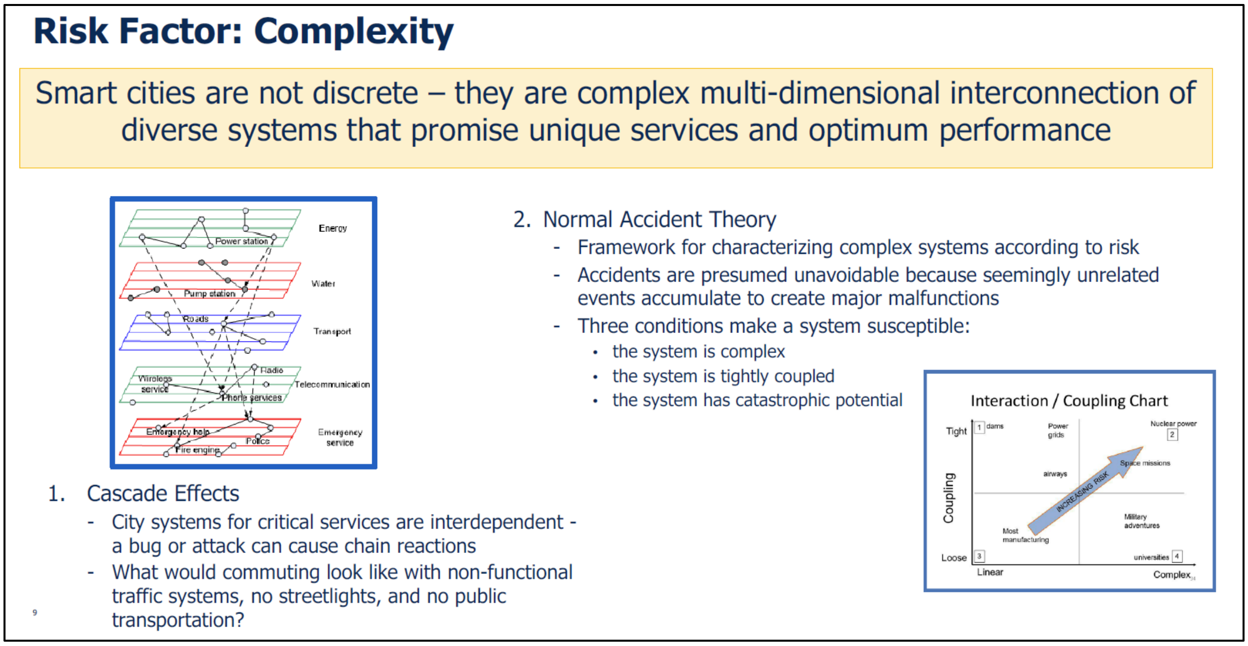
5.6 Conclusions and Next Steps

Smart Cities are solving the problems of today with an eye on the future by adhering to roadmaps that address pressing issues while still making sound financial sense. IoT technology drivers and conditions of necessity described in the use cases will transform today's IoT revolution into the norm of tomorrow. Of course, there will be successes and failures in areas of hardware, software, networks and societal acceptance along the way, but like all ecosystems, the better practices will thrive and achieve equilibrium.

The major roadblock standing in the way of Smart Cities and, more generally, IoT technology deployment will remain the possible breakdown of the benefits model, i.e., delivery at odds with the promises. Data breaches, unwarranted invasion of personal privacy, misuse of information, process opacity and/or lack of user/citizen focus could cast a shroud of suspicion and doubt over the purported advantages and, as a result, significantly delay IoT acceptance and progress.

Today, many solutions live within an independent (idiosyncratic) cluster that does not allow open connectivity throughout the overall IoT ecosystem. Interconnecting all things will necessitate having the ability to connect all applications and devices easily and cost-effectively with standards and platform agreements including proper governance ensuring security and safeguarding privacy.

As far as Smart Cities, the intrinsic complex interdependence of the various building blocks requires an overarching (holistic) modus operandi (see Figure 21).



Risk Factor: Complexity

Smart cities are not discrete – they are complex multi-dimensional interconnection of diverse systems that promise unique services and optimum performance

1. Cascade Effects
   - City systems for critical services are interdependent - a bug or attack can cause chain reactions
   - What would commuting look like with non-functional traffic systems, no streetlights, and no public transportation?
2. Normal Accident Theory
   - Framework for characterizing complex systems according to risk
   - Accidents are presumed unavoidable because seemingly unrelated events accumulate to create major malfunctions
   - Three conditions make a system susceptible:
     - the system is complex
     - the system is tightly coupled
     - the system has catastrophic potential

Figure 21: Complexity and Interdependence of Smart City Systems[255]

[255] Dr. Margaret L. Loper, "Trusting Smart Cities: Risk Factors and Implications," presentation at the Mad Scientist Conference: Installations of the Future, op. cit. The chart on interaction/coupling is from David Etkin

6 KEY INSIGHTS AND LOOKING FORWARD

The Internet of Things is a “system of systems”, as illustrated in Figure 22 below from NIST.

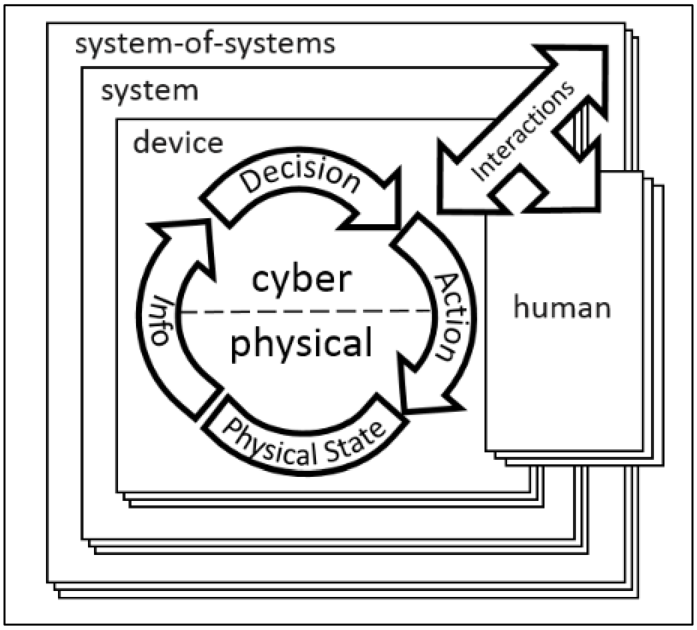


Figure 22: Cyber-Physical Systems [CPS] (IoT) Conceptual Model[256]

It weaves in multiple new and existing devices, networks, organizations, and use cases. It follows that all stakeholders need to collaborate in order to define priorities and optimize the use of infrastructure and capabilities serving citizen needs.

In spite of substantial progress, there has yet to be a single established IoT architecture (examples of leading related efforts currently underway are highlighted in section 1.2). Instead, there are scores of complementary and competing configurations for system designs.

and Peter Timmerman, “Emergency management and ethics,” International Journal of Emergency Management, January 2013, (“Figure 2 -- The four quadrants of normal accident theory, as a function of complexity (x-axis) and coupling (y-axis),” p. 285), (9(4):277 – 297 available at https://www.researchgate.net/publication/264812137_Emergency_management_and_ethics . The city layered model is from P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, “Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research,” Idaho National Laboratory, August 2006, (“Figure 1 – Infrastructure Interdependencies,” p.3), available at http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf. Regarding collaboration and integration in Smart Cities, see: T.J. Becker, “Smart Cities,” Georgia Tech Research Horizons, Issue 1, 2017, http://www.rh.gatech.edu/features/smart-cities

[256] NIST, Framework for Cyber-Physical Systems, Release 1.0, op. cit., p. 6

Integrated IoT systems can be more effective and efficient than if implemented separately, in parallel, and in silos. This applies even more in the case of Smart Cities.

With this increased collaboration, however, data ownership is of paramount importance; in most cases the IoT value lies in the data.

Since IoT is about interconnecting intelligent things, much of the raw data will be scrubbed and processed by smart devices before being passed on to other entities. Then; who owns this processed output? Is it the owner of the original data; the owner of the algorithm that processed it; and/or other stakeholder? It is about to become a "very big deal"![257]

Security (section 3.2) and privacy (section 5.2) issues have rapidly become the most debated topics in the Internet of Things arena. IoT adoption for given solutions and society as a whole rests on robust security and tight privacy.

Given the widely spread negative publicity of data breaches and IoT malware (section 1.2), even the perception of vulnerability or unmitigated risk causes an uneasiness among potential adopters that is detrimental to IoT expansion.

The nature and intensity of these challenges call for major adjustments and progress in a variety of disciplines and fields including not only engineering[258], but also law[259],

[257] Paul Gilin, "Who owns data from the 'internet of things'? That's about to become a very big deal," SiliconAngle, October 15, 2017 https://siliconangle.com/blog/2017/10/15/owns-iot-data-thats-become-big-deal/. Note that not only data ownership is a challenge, but so is the embedded software ownership. See this insightful article on the topic: Mulligan, Christina, "Personal Property Servitudes on the Internet of Things," (July 14, 2014). 50 Georgia Law Review 1121 (2016); Brooklyn Law School, Legal Studies Paper No. 400. Available at SSRN: https://ssrn.com/abstract=2465651 or http://dx.doi.org/10.2139/ssrn.2465651. Professor Mulligan's paper addresses the legal, economic and social issues surrounding the terms of service (ToS) or end-user license agreements (EULAs) from manufacturers of networked (IoT) objects, which impose restrictions on how the products can be used or transferred.

[258] Jennifer Bosavage, "How the Internet of Things Will Impact Engineering Careers - New opportunities abound for those in software, mechanical, and manufacturing," The Institute, IEEE, February 14, 2018 http://theinstitute.ieee.org/technology-topics/internet-of-things/how-the-internet-of-things-will-impact-engineering-careers

[259] For instance, the current Fourth Amendment doctrine, i.e., about "*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*" may need to evolve to take into account the Internet of Things. See Ferguson, Andrew Guthrie, "The Internet of Things and the Fourth Amendment of Effects," (August 3, 2015), 104 Calif. L. Rev. 805 (2016), available at SSRN: https://ssrn.com/abstract=2577944. Ferguson submits*: "How the Fourth Amendment adapts to these new sensor surveillance systems [Internet of Things] will be a central issue in the coming years."* See also additional perspectives on the same topic *"to protect the data trails we leave behind"* in Andrew G. Ferguson, "The Smart Fourth Amendment,", 102 Cornell L. Rev. 547 (2017) Available at: https://scholarship.law.cornell.edu/clr/vol102/iss3/1. The American Bar Association (ABA)'s Section of Science and Technology Law's *Internet of Things National Institute* annual conferences share insights and practical guidance on the "escalating legal risks of doing business in a connected world," see for example the program of the May 2018 conference http://www.iotjournal.com/articles/view?13003/

regulation[260], policy[261], business[262], education[263] and training[264]. These changes must be broad and deep since IoT is here to stay.

The Internet of Things is for the long haul[265].

We expect IoT will grow in clusters, where various use cases and their related devices, applications and connectivity shape their ecosystem. While these clusters begin to arise, there will be a natural tendency for them to try to link first to other like clusters. As "clusters of clusters" start to crystallize, standards and regulations will emerge to enhance their ability to work together on a common platform.

Smart Cities/IoT deployment roadmaps will differ based on location and other factors (demographics, economics, etc.), e.g., from a major city in a developing country to a megalopolis in a developed country. However, they all should bear a common thread of responsible digital governance (enabling the citizens to have effective control of their digital life) and sustainability (control of the environment) while allowing municipal governments and business partners to extract necessary and reasonable social and economic value (section 4.3) from their investment in money, time and people.

[260] It has been argued, "the rise of the Internet of Things will challenge regulatory structures" and may bring about "code as law" and "governance by things" – see Wolfgang Schultz and Kevin Dankert, " 'Governance by Things' as a challenge to regulation by law,' Internet Policy Review, June 30, 2016 https://policyreview.info/articles/analysis/governance-things-challenge-regulation-law. "Algorithmic Regulation", a term coined by Tim O'Reilly, is a closely related concept (see http://beyondtransparency.org/chapters/part-5/open-data-and-algorithmic-regulation/, especially the section on "the role of sensors in algorithmic regulation.") A recent review of algorithmic regulation is provided by University of Birmingham (U.K.) Professor Karen Yeung here: Yeung, Karen, "Algorithmic Regulation: A Critical Interrogation," (May 23, 2017). TLI Think! Paper 62/2017; Regulation & Governance, Forthcoming; King's College London Law School Research Paper No. 2017-27. Available at SSRN: https://ssrn.com/abstract=2972505

[261] See Courtney Bjorlin, "In driving digital transformations, watch government policy," Internet of Things Institute, November 29, 2017 http://www.ioti.com/industrial-iot-iiot/driving-digital-transformations-watch-government-policy; and U.S. Department of commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017 https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[262] Scott Amyx, "Internet of Things' impact on business: Major overhaul ahead," Internet of Things Institute, July 6, 2017, http://www.ioti.com/strategy/internet-things-impact-business-major-overhaul-ahead

[263] See Barry Burd, Ata Elahi, Ingrid Russell, Lecia Jane Barker, Félix Armando Fermín Pérez, Bill Siever, Monica Divitini, Alcwyn Parker, Liviana Tudor, and Jorge Leoncio Guerra Guerra, "The Internet of Things in Computer Science [CS] Education: Current Challenges and Future Potential,"
Proceedings of the 2017 ACM Conference on Innovation and Technology in Computer Science Education, July 3-5, 2017, https://dl.acm.org/citation.cfm?doid=3059009.3081331

[264] See P.K. Argawal, "IoT Skill Shortage Ahead," EETimes, November 28, 2017 https://www.eetimes.com/author.asp?section_id=36&doc_id=1332655 and report on "Optimism and Anxiety: Views on the Impact of Artificial Intelligence and Higher Education's Response," based on a survey conducted in 2017 by Gallup and Northeastern University, January 2018, https://news.gallup.com/reports/226475/gallup-northeastern-university-artificial-intelligence-report-2018.aspx

[265] Alain Louchez, "The Internet of Things is a Secular Transformation," IoT Journal, May 4, 2015 http://www.iotjournal.com/articles/view?13003/

Whether it is within a Smart City or any other IoT context, the key to success is to ensure all stakeholders are and feel aligned with clearly spelled out goals.

Integral to the quality of the citizen engagement are the funding (e.g., public tax dollars) and financing (e.g., debt issuance) of the IoT projects (section 5.3). Since cities cannot go it alone, IoT investments will likely lead to new forms of partnerships and business models[266]. In the meantime, cities may find it wise to develop small-scale pilot projects as opposed to "Big Bang" implementations (section 5.5) for concept proofing and risk minimization.

Being clear and transparent from the outset will go a long way in getting acceptance and support.

By focusing on universal design[267]; stakeholder involvement; security and privacy by design; and economic and social feasibility, as well as sustainability, Smart Cities' IoT implementations will be successful through fostering meaningful citizen engagement; and meeting the needs of all parties involved[268].

[266] See Bee Smart City, "Paying for Smart Cities: Where's the Money", January 24, 2018, https://hub.beesmart.city/strategy/paying-for-smart-cities-wheres-the-money*: "To make progress, cities need to carefully consider the cost-benefit of any investment as well as exploring new finance and funding models. One thing is certain: it's unlikely cities can go it alone."*

[267] Dr. Helena Mitchell, Regents' Researcher and Executive Director of the Center for Advanced Communications Policy (http://cacp.gatech.edu/) at Georgia Tech; a Principal Investigator of the Rehabilitation Engineering Research Center for Wireless Technologies(http://www.wirelessrerc.gatech.edu/); and a member of the Federal Communications Commission's disability advisory committee (*) *"argues that companies should embrace the principles of universal design—that is, creating products and services everyone can use and that are, ideally, universally compatible. Having such an approach could actually make more financial sense in the long run. 'What you don't want is to have to retrofit for a population you forgot about,' Mitchell says. It may also uncover unintended client bases; for instance, a connected device to help people with low vision could also potentially help improve firefighters' vision when entering a smoke-filled building. Still, there are many real and perceived barriers to innovating for disabilities. One of the problems Mitchell hears most often from companies is that they don't know how to reach enough people with disabilities to test a product. She urges companies to partner with universities to design, create and test new products. University research departments often have long lists of potential focus-group participants who could serve as product testers. And, Mitchell continues, schools also have labs and R&D groups that are far cheaper to hire and staff than creating a private lab. Another option is to partner with veterans' groups, as many war veterans have acquired disabilities. Governments also need to take a broader role in starting, and maintaining, the conversation about designing for disabilities, Mitchell says. She doesn't advocate for government setting industry standards—by the time a standard is created, the technology will be outdated. 'I'm more for looking at social and cultural aspects of designing next-generation technology,' she says. 'It becomes a question of, what do people with disabilities use the most now, and how can it benefit all users?'* in Tracey Lindeman, "Innovating for people with disabilities: Why companies should invest in universal design," IBM Blog ("insights on business"), June 25, 2017, https://www.ibm.com/blogs/insights-on-business/ibmix/innovating-people-disabilities-companies-invest-universal-design/ Lindeman, "Innovating – (*) See FCC disability advisory committee (DAC)'s recommendations on IoT dated December 6, 2016 here: https://www.fcc.gov/document/dac-recommendation-internet-things

[268] IoT.ATL is an example of a Smart City-centered initiative that aims to develop "the right kind of ecosystem and business environment in place to foster innovation." See Adina Solomon, "Atlanta hopes to become global leader in internet of things technology," Crain's, April 9, 2018 http://www.crains.com/article/news/atlanta-hopes-become-global-leader-internet-things-technology

In May 2016, members of the Internet of Things Council offered their views on the future of the Internet of Things. Their perceptive comments remain useful guideposts in 2018:

> *"As with any technology that is as hyped as the IoT, there involuntarily comes a slowdown in interest when the realisation sets in that it will take more time than expected, is more complicated to execute, and that there are significant risks associated with it (which were simply brushed away during the euphoric phase that any hype starts off with) /…/ The IoT is not just a new paradigm, it is a new world order, not so much in the political sense but in the nature of the term: 'order' as in 'hierarchy', reciprocity and communicative relations. We are entering a world in which the environment becomes the interface, and there will be no more dual relations (me and you, me and an object), but there will be always a third party (sensor-database) involved."*[269]

As we are looking back on IoT's initial steps, and trying to discern what lies ahead, it is hard to refute that, around the world, a lot has been accomplish to build a solid foundation for future expansion with multifaceted benefits. In the process, enthusiastic eagerness may have distorted expectations, especially regarding timeframes.

However, until now, the Internet of Things has just been revving up its powerful engine, admittedly with a lot of noise.

The next decade should be decisive as roadblocks are progressively overcome, and IoT technologies become inescapably, pervasively and tightly entwined into the economic and societal fabric.

We expect IoT will grow in clusters, where various use cases and their related devices, applications and connectivity shape their ecosystem. While these clusters begin to arise, there will be a natural tendency for them to try to link first to other like clusters. As "clusters of clusters" start to crystallize, standards and regulations will emerge to enhance their ability to work together on a common platform.

[269] Alexander Grankin, Damir Caušević, Gérald Santucci, Harris Moysiadis, Rob van Kranenburg, and Toby Ruckert, "Europe's IoT," Pan European Networks - Issue 18, May 2016, https://www.theinternetofthings.eu/sites/default/files/GOV18%20R%20van%20Kranenburg%206007_ATL.pdf

7 About CDAIT

The Center for the Development and Application of Internet of Things Technologies (CDAIT, pronounced “sedate’) is a global, nonprofit, partner-funded center located in Atlanta, GA that fosters interdisciplinary research and education while driving general awareness about the Internet of Things (IoT).

CDAIT bridges sponsors with Georgia Institute of Technology (Georgia Tech) faculty and researchers, as well as industry members with similar interests.

Central to its value proposition is the belief that only a holistic approach, i.e., mindful of the complexity of the entire IoT value chain and the intricate relationships between the various links, can generate superior results. CDAIT’s broad overarching goal is to expand and promote IoT’s huge potential and transformational capabilities.

Anchored at the Georgia Tech Research Institute (GTRI), a highly regarded applied research and development organization with a global impact and focus on real-world research for government and industry, CDAIT is backed by Georgia Tech’s diverse and distinguished community of faculty and researchers. CDAIT aims to efficiently identify, understand and solve challenges and problems that may arise along the entire Internet of Things value chain through six Working Groups: IoT Education and Training; IoT Startup Ecosystem; IoT Thought Leadership; IoT Security and Privacy; IoT Standards and Management; and IoT Research.

For more information, including the current membership list, visit https://cdait.gatech.edu.

8 CDAIT Leadership

Alain Louchez
Co-founder & Managing Director
alain.louchez@gtri.gatech.edu

Jay Sexton
Chief Operating Officer
jay.sexton@gtri.gatech.edu

Margaret Loper, Ph.D.
Chief Technology Officer
Margaret.loper@gtri.gatech.edu

Jeff Evans
Co-founder & Chair of Executive Advisory Board
jeff.evans@gtri.gatech.edu

9 CDAIT IoT Thought Leadership Working Group

While there are many technological challenges that are inherently tied to the development of the Internet of Things (IoT), there are also a number of non-technological, yet critical, issues that must be addressed for IoT to succeed at any level. The CDAIT IoT Thought Leadership Working Group is tasked with exploring these dimensions and hurdles, which are rooted in the radical business, economic and societal transformation the Internet of Things is bringing about. Business models; monetization; technology awareness, acceptability, and accessibility; and ethical, legal, policy and regulatory frameworks are only a few examples of such potential research areas. This is a multidisciplinary undertaking, which encompasses a host of perspectives, including especially those found in social sciences and humanities. By focusing on these crucial issues, the IoT Thought Leadership Working Group strives to ensure IoT is implemented in a seamless, sustainable, and impactful way.

10 CONTRIBUTORS - IOT THOUGHT LEADERSHIP WORKING GROUP

Karen I. Matthews, Ph.D., Chairperson
Technology and Market Development
Manager, Science and Technology
Corning Incorporated

Paul M.A. Baker, Ph.D., Vice-Chairperson
Senior Director, Research and Strategic
Innovation, Center for Advanced
Communications Policy
Georgia Tech

Clay Mahaffey, Vice-Chairperson
Global R&D and Innovation Director
Kimberly-Clark

Forrest Pace, Vice-Chairperson
Senior Underwriter Property & Casualty -
Cyber & Strategic Risk Leader
AIG

Kelly Arehart
Senior Manager, Global Innovation
Kimberly-Clark

Steven Becker
Global Leader - Open Innovation & Integrated
Solutions Architecture
Kimberly-Clark

Ryan Dooley
Senior Product Manager for IoT
AIG

Sri Elaprolu
Public Sector IoT
Amazon Web Services

Doug Guthrie
Senior Vice President, Big South Region
Comcast

Jerome Holbus
Senior Product Manager, IoT
Infor

Ganesh Kashyap
Vice-President, Strategic Delivery
Landis + Gyr

Marvin Laster
IT Senior Architect
IBM

Thiago D. Olson
Managing Director
Engage Ventures

Johnny Parham
Solutions Architect
Infor

Mallie Eric Preston
Global Practice Leader - IoT Solutions Group
AT&T Mobility

Rick Purcell
Engineering Technical Leader
Kimberly-Clark

Gloria Rismondo
Product Strategy and Management
Professional
Global Payments

Adam Rykowski
Vice President of Product Management,
Unified Endpoint Management
VMware

Jay Sexton
Chief Operating Officer
CDAIT
Georgia Tech

Jonathan Staab
Director, Product Management
Communications Networks
Landis + Gyr

Georgia Tech | Center for the Development and Application of Internet of Things Technologies

cdait.gatech.edu

75 5th Street NW, Suite 900
Atlanta, Georgia 30308