Community Mesh Networks: Citizens Participation in the Deployment of Smart Cities

Primavera de Filippi

Community Mesh Networks:
Citizens Participation in the Deployment of Smart Cities

Primavera De Filippi
CERSA/CNRS/Université Paris II - Berkman Center for Internet & Society at Harvard

Abstract

Smart cities embed information and communication technologies (ICT) to create interactive milieus that constitute a bridge between the physical and the digital world. In their attempt to improve citizens' quality of life through a more efficient use and sustainability of resources, smart cities might, however, also raise important concerns as regards the privacy and confidentiality of personal data flows.
Insofar as the design of a city's telecommunication infrastructure is likely to affect the nature of social dynamics and human interactions, it should, ideally, be achieved through a coordinated, citizen-centric approach combining integrated ICTs with active citizen participation and an intelligent management of physical, digital and informational resources. This chapter analyzes the case of community mesh networks as an example of grassroots decentralized communication infrastructures, whose architecture design has important implications on the deployment and configuration of smart cities.

Keywords: Internet infrastructure, surveillance, P2P networks, participatory design, citizen activism

Key Terms and Definitions:

- *Smart cities*: Smart cities embed information and communication technologies (ICT) to create interactive environments that constitute a bridge between the physical and the digital world. People interact with these environments by means of physical artifacts (sensors, smart devices, etc) powered by the computational power of the network to which they are connected. In their attempt to increase the quality of life through a more efficient use and sustainability of resources, smart cities raise, however, important concerns as regards the privacy and confidentiality of personal data flows.
- *Information or data privacy*: The right to privacy refers to the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. Specifically, in line with the definition provided by the European Charter of Fundamental Rights, the right to privacy is to be distinguished from the fundamental right to data protection, which is more concerned with the manner in which personal data is being collected and processed.
- *Information or data security*: In computing, security is commonly described as the conjunction of three major properties: information confidentiality (the fact that only authorized entities can access a piece of information), integrity (the fact that a piece of information cannot be unduly modified) and availability (the fact that authorized entities are not prevented from accessing a piece of information). In order to ensure these properties, various types of properties and technical tools may be used, such as authentication, authorization, non-repudiability, encryption, cryptographic signature, etc.
- *Cloud computing:* Cloud computing refers to a distributed infrastructure that is made of a collection of interconnected computers, whose resources are pooled together into a virtual machine that maintains and manages itself. As opposed to other distributed architectures, the particularity of cloud computing is that the architecture is completely independent from the physical infrastructure it relies upon. This allows for extreme flexibility, as resources can be dynamically added or removed according to actual needs.
- *Peer-to-peer Networks:* Peer-to-peer networks are decentralized network infrastructures that rely instead on a distributed system of communication based on a more symmetrical (non-hierarchical) model. As opposed to the traditional client-server approach to network communications, peer-to-peer network architectures rely on a network of peers that act both as clients and servers, depending on the circumstances.
- *Mesh Networks:* Mesh networks are decentralized network infrastructures that rely on a distributed and loosely coordinated network of peers contributing their own resources to the network so as to provide Internet connectivity to a specific community without relying on any pre-existing network

infrastructure. They are more robust than traditional centralized networks, in that they can dynamically adapt to changes in their surroundings and automatically reconfigure themselves according to the current availability of resources.

Introduction

Smart cities aim at promoting economic development, sustainability, efficiency and greater quality of life (QoL) by using modern digital assets and mobile communication technologies to provide new and innovative services directed towards fulfilling old and emergent citizens needs by encouraging participatory action and civil engagement (Caragliu &. al, 2009). As such, the deployment of smart cities is a complicated task that involves many multi-faceted issues, comprising questions such as environmental and infrastructural design, community living, and individual mobility. Many different stakeholders are involved in the process of turning a city into a smart city, yet the ultimate beneficiary is (or should be) the citizen. Thus, in order to succeed, this process should, ideally, put citizens at the center of the analysis, considering them as agent, rather than mere target (Nam & Pardo, 2011).

After providing a general overview of the traditional approach to smart city deployment, this chapter analyses the arguments behind the severe criticism which smart cities have recently been subject to. On the one hand, there is a growing mistrust towards a mere technologically-driven approach to smart cities, which tend to be treated as an end *per se*, rather than as a means to provide better services and greater QoL to their citizens. Rather than looking at the consequences that technology might have on the social dynamics and perceived interests of people inhabiting the city, the focus is often excessively geared towards improving the technical infrastructure of the city, whose inhabitants are mainly treated as passive users rather than pro-active citizens (Humphries, 2013). On the other hand, the data-driven character of many smart cities - collecting personal information about citizen's habits, lifestyles, and keeping track of their daily behaviours - raises important concerns as regards the privacy and confidentiality of personal data. To the extent that such data is collected, stored and processed by third party operators, citizens lose control over their own personal data, which may be used for secondary purposes without the consent of the data subject (Martinez-Balleste, 2013).

In this context, after the first run of experiments with smart cities deployment (see e.g. the several initiatives in Tokyo, London, New York and Barcelona, Singapore's Intelligent Transport System, Dubai's Internet City project, and more recently, South Korea's Ubiquitous-City project to turn the city of Incheon into the world largest and most hi-tech smart city) has shown that a socially-oriented design to urban development is a critical requirement that could lead to dangerous outcomes if not properly implemented. Indeed, if the needs of citizens are not properly taken into account in the development of smart cities, the outcome is likely going to be an environment that actually alienates the citizens who do not recognize, nor understand (and sometimes simply do not agree with) the new value propositions that are being offered to them through the smart city infrastructure. Given the growing impact that technology is having on our everyday life, there is, today, a growing need to implement smart cities through a more grassroots, citizen-centric approach.

Emerging technologies may provide a solution to that need, by facilitating the development of tools for promoting social inclusion and participation in the design of tomorrow's smart cities. This chapter focuses specifically on the use of mesh networking technology as an example of grassroots decentralized communication infrastructures that could play an important role in deployment of smart cities. The objective is to understand whether, and how, can citizens become active participants in improving their own city's infrastructure, without renouncing to their own individual autonomy, nor foregoing their rights to privacy and data protection. Ultimately, the success and long-term sustainability of smart cities might, indeed, depend more on their ability to deploy new and innovative instruments for the empowerment of communities, rather than on the deployment of sophisticated technologies which are deployed and controlled by third party operators, and subsequently imposed in a top-down fashion to the city's inhabitants, without giving them the opportunity to participate to the design and management of these technologies. If the goal is, ultimately, to improve the quality of citizens' life, it is not enough to supply more personalized and customized services, it is also important – if not essential – to provide citizens with new opportunities for social interactions within the urban environment, along with a higher degree of freedom and autonomy.

Background

Smart cities embed information and communication technologies (ICT) to create interactive environments that constitute a bridge between the physical and the digital world. Technological advances are pushing towards digital convergence. As different media can now communicate with one another, an increasing number of devices and applications are becoming more and more integrated, and dependent upon each other. Digital technologies are slowly finding a place into our everyday's objects and devices, increasingly blurring the line between the physical and digital world.

The deployment of high speed broadband allows for expeditious communications and facilitates the global dissemination of large amounts of information, in virtually no time. Wireless networks have brought connectivity to a whole new level by enabling mobile devices to remain connected to one another, even when in transit. This allows for the establishment of dynamic network connections which can be easily shared amongst multiple devices at virtually no costs. Thanks to the proliferation of smart phones and other mobile devices, individuals are always connected and constantly communicate -- either consciously or unconsciously -- with the digital world.

We have today entered a new era of ubiquitous and pervasive computing. Computers, laptops, tablets, smart phones or other digital devices are increasingly connected (and interconnected) in such a way as to able to communicate and exchange information with one another (Want & Pering, 2005). In the most industrialized countries, it is nowadays difficult for people to communicate in such a way that does not involve any modern telecommunication network or digital device. People are increasingly connected to each other through their own devices -- which are, in turn, connected to many other people or devices.

With the advent of cloud computing, individuals are now capable of accessing their own data (including their personal data) regardless of their physical location and without being tied to any specific device. Smart (connected) devices are becoming a *de facto* standard, or simply a necessity in such an information-driven society, where most of the utility or use value is no longer derived from the use of the device itself, but rather from its ability to connect with the networked digital world. Connectivity has, eventually, become an essential prerequisite to the information infrastructure of any modern city.

In the age of ubiquitous computing, smart devices become an integral - and yet, often invisible - part of the world we live in (Steventon & Wright, 2006). With the Internet of Things (IoT), the Internet extends its reach to the physical world. Connected devices are turned into sensors that automatically collect data and record changes in users' behaviors, sometimes without them even being aware of it. Individuals are surrounded by sensors of all kinds: personal computers, smartphones, or other integrated devices (including objects such as kettles or fridges, but also more personal accessories, such as clothing, bracelets, or watches) are now equipped with Internet connection, positioning tracking systems, accelerometers and even RFID readers. These devices are constantly tracking and recording information about the world surrounding them, in order to learn more about users' activities and behaviors, as well as their specific preferences and tastes. With the recent growth in popularity of the 'quantified self' community -- individuals interested in monitoring or self-tracking themselves by means of wearable sensors and devices -- the amount of data available on the Internet is now greater than ever (Swan, 2012).

These large quantities of data are being continuously aggregated, processed and analyzed in order to produce new information, with a growing level of accuracy. In the context of smart cities, this often leads to more customized or personalized services that ultimately contribute to increasing citizens' quality of life (Brooks, 2013).

To date, intelligent sensors have already been deployed in a variety of cities, in order to support and facilitate the management of daily tasks, in a costless and much more efficient way. For instance, the City of Westminster has installed sensors in parking spaces to help drivers find parking in nearby streets. In Barcelona, waste containers have been equipped with sensors that communicate the container's state to waste collectors, so as to promote a more efficient and dynamic route management system for waste collectors (who can focus exclusively on the containers that are full, while ignoring those that do not need to be collected). Always in Barcelona, sensors have been deployed in certain areas of the city to modify the intensity of street lights, not only according to meteorological conditions, but also depending on the density of people in public squares.

While this might seem trivial at first, the combination of these small enhancements into a more integrated ecosystem could lead to the establishment of a much more sophisticated system, made of a multiplicity of

interconnected parts interacting with one another in a dynamic way, so as to adjust their operations according to the information they receive from the other components of the system. As more and more facets of our world are turning into data, the urban environment becomes, itself, part of the global information system, eventually leading to the creation of hybrid environments -- “phygital” spaces merging the physical world with the digital world by means of electronic artifacts powered by the computational power of the network to which they are connected (Bazzanella & al., 2013).

Infrastructure design and its social implications in the context of smart cities.

Connectivity, ubiquity and interactivity are key elements to the design of a city's socio-technical infrastructure. Modern telecommunication infrastructures make it possible for the municipality to manage large complex environments and to better communicate with its citizens. Intelligent sensors deployed in a networked environment allow for a more efficient use or resources -- whose usage can be more easily monitored and administered from afar. As digital technologies are incorporate into most of the infrastructures of communication, the city becomes more responsive to current and emerging citizens' needs. Indeed, not only does the entanglement of digital technologies within the urban space enable a more responsive reaction to disruption (e.g. power outage, floods, traffic or congestions, etc), it also provides the means to collect and process large amounts of data from present and past situations, so as to anticipate real-world problems or events.

Smart cities constitute a platform for creating new services that rely on collective intelligence to offer innovative solutions to citizens' needs. By turning the urban space into a more dynamic and interactive environment, the IoT represents an essential step towards the establishment of a more modern and efficient city management system. The challenged raised by rapid technological changes and emerging users' needs requires the creation of an intelligent environment made up of a network of integrated devices communicating with one another, so as to provide citizens with highly customized and personalized services, before they even feel or express the need for these services.

All this, however, comes at a cost. To the extent that these communication infrastructures determine the nature of social dynamics and human interactions, their benefits cannot be properly understood without accounting for the possible repercussions they might have on citizens' social and civic life. In this regard, the architectural design of these infrastructures must be carefully scrutinized when analyzing the impact they have on civil liberties and democratic values. This is all the more relevant when it comes down to the privacy of end-users, which is currently being jeopardized by the systematic collection of personal data or information that we are witnessing today on the Internet. In such any data-driven society, preserving the privacy and confidentiality of personal data flows becomes a crucial issue, which might lead to a series of unpleasant consequences if it is not properly accounted for. In order to fully exploit the potential of smart cities, in accordance with the fundamental rights of end-users, the design of their telecommunication infrastructure needs to be carefully taken into account, both at the conception and during the overall deployment of the urban environment.

1. Centralized and decentralized network infrastructures

The design of any given infrastructure shapes or influences the social dynamics that might occur on that structure -- *i.e.* it affects the ways in which people interact with and through that structure. In the context of communication infrastructures, the design determines the nature of information that is communicated throughout the network (e.g. voice, video, data, etc), the way such information is imparted to the public (one-to-one, one-to-many, many-to-many), and the way different information agents can interact to each other (centralized, hierarchical structures vs. distributed, symmetrical organisations). Different typologies of network architectures might, therefore, encourage or discourage different types of communications and information flows.

Centralized network infrastructures are likely to promote the deployment of hierarchical communication systems, whereby individuals have to connect to one or more established servers in order to gain access to a particular network. This is the model adopted by standard TV and radio broadcasting (one-to-many), traditional telephone communication systems (where all communication have to pass through at least one telecommunication operator) and most Internet service providers implemented thus far. In spite of their differences in function and scope, all of these infrastructures share an important commonality: they all rely on a centralised entity in charge of regulating access to the network and managing the information flow travelling on that network.

Decentralized network infrastructures rely instead on a distributed system of communication based on a more symmetrical (non-hierarchical) model. As opposed to the former client-server approach to network communications, decentralized architectures rely on a network of peers that act both as clients and servers,

depending on the circumstances. Every node in the network is equally important (although the model might allow for supernodes, which have priority over the other nodes) and they all contribute to managing access and routing traffic through the network of peers.
This model is inspired from the advent of distributed applications designed to allocate tasks and workloads amongst a network of peers, first popularized with the deployment of P2P file sharing applications. Yet, the model inspired people to experiment with decentralized structures in many other areas of human interaction -- from software development with the open source movement (Healy & Schussman, 2003), to artistic production with Creative Commons licenses (Lessig, 2004; Benkler, 2006), and, more recently, the implementation of decentralized monetary systems, such as Bitcoin and other derivative crypto-currencies (Nakamoto, 2008).
P2P systems challenge most of the dominant practices associated with centralized environments. Firstly, they eliminate the need to establish a hierarchical structure by establishing a network of peers which are all assumed to be equal. Secondly, they eliminate the need for intermediaries, thus bypassing the traditional bottlenecks characteristics of centralized production processes. Thirdly, they promote an alternative model of production which relies on sharing and cooperation as preconditions for the viability and long-term sustainability of the system. This latter point brings along a wide set of social implications due to the human dynamics associated with peers collaboration. In this sense, P2P systems also represent a political choice (Bauwens, 2005), to the extent that they rely on specific social and relational ties between all participants involved in decentralized production, which ultimately promotes a specific organisational and political structure.
As illustrated by Raymond's topical paper "*The Cathedral and the Bazaar*" (1999), as opposed to traditional models of production based on a top-down approach to decision-making, where only a few people are in charge of, and responsible for the implementation of a project according to specific rules and constraints (e.g. the *Cathedral* model), the *Bazaar* is characterised by a much more grassroots and bottom-up approach, which distinguishes itself to the extent that the production processes are not dictated by any single entity, but rather by the project itself. In other words, a community of dispersed individuals contribute to the project not because of a specific commitment they have made, but merely because of their shared view and commitment to achieving a common objective. The system of norms regulating this latter type of production is therefore extremely informal, often based on the principles of *actocracy* (*i.e.* the first to act is the one to rule), collective agreement and implicit consensus (O'Mahony & Ferraro, 2007). Everyone willing to participate can contribute to the project, and, by doing so, becomes an integral part of the decision-making process.
Although the Bazaar governance model has thus far mostly been tested in the context of online communities concerned with the production of digital, non-rival goods (software, content, data, etc), several attempts have been made to export this particular system of governance to other fields of endeavor. The following sections illustrate the privacy-deficit that is characteristics of a large number of smart city environments whose design is grounded in a centralized architecture, to analyse, subsequently, the case of community mesh networks as an example of how the mechanisms of decentralized governance and P2P production can be implemented at the level of the technical infrastructure of communication. This is an excellent example of innovation and privacy working hand in hand, as privacy is embedded into the design, operation, and management of the communication infrastructure, across the entire information lifecycle.

2. The Issue: Privacy and Data Protection

Security, privacy and confidentiality play a key role in the design of smart city infrastructures. Yet, preserving individuals' privacy and autonomy in the context of smart cities is today an arduous challenge, in particular in light of today's efforts at generalized surveillance by both corporate and governmental entities (Bauman & Lyon, 2012).
While they involve the deployment of a large number of sensors distributed throughout the whole city, the information management system adopted by a large majority of smart cities are, generally, highly centralized. Huge amounts of data (from air temperature to air contamination, or carbon dioxide levels, from electricity usage to gas, humidity, or dew point, from current street traffic to available parking spaces, etc) are collected and aggregated into large centralized data centers, where they are subsequently processed - through sophisticated algorithm and big data analysis techniques to identify the current concerns or foresee the upcoming ones, and perhaps figure out the causes or solutions to the various issues affecting the city.
Most of these initiatives have, however, been launched with a view to increase the overall efficiency of

public services, without paying too much attention on their implication on the privacy of individuals -- eventually leading to a state of ubiquitous surveillance that is similar (or worse) than the one currently found on the Internet.

On the Internet, mass surveillance has become a critical issue, especially after the Snowden's revelations concerning the operations of the U.S. National Security Agency (NSA), which gave a symptomatic example of the intrusive powers that governmental bodies are exerting in the digital world. Increasingly sophisticated technologies (such as sniffers, spoofers, keyloggers, or Deep Packet Inspection techniques) are currently being employed by both private parties and public authorities to monitor online communications.
While such practices have been performed for many years over the Internet, they are now also emerging in the physical world. In fact, they have been greatly amplified with advent of smart cities and the IoT, which combine urban management with pervasive computing, ubiquitous networks and distributed sensors connected to each other into order to provide real-time information about the world around us.
Today, as more and more devices are connected to the Internet network, surveillance is progressively extending to every aspect of our daily life. Our digital footprints are getting bigger and bigger (Madden, 2007), as everywhere we go, everything we do, and everything we interact with - either online or offline - is collecting data about us. A striking example is the rapid deployment of surveillance cameras (CCTVs), which were initially deployed only in the context of specific locations, such as shopping malls or business complexes, but are progressively taking over the public landscape of many metropoles around the world (such as London, Hong Kong, Singapore, etc). These cameras no longer operate on their own, they are more and more integrated with other sensors and control systems, such as fire detectors, alarms, and anomalies detectors, but also traffic control system, crowd flow monitoring, forecasting stations, and so forth. As more and more connected sensors permeate the urban territory, they might progressively lead toward the establishment of effective command and control systems (such as the one temporarily deployed in the context of large-scale demonstrations or sports events) to be permanently deployed at the city-level so as to get a better picture of citizens activities within the urban landscape. This trend can already be observed in several smart cities, such as the Domain Awareness Center[1] in Oakland, California, or Rio de Janeiro's Intelligent Operations Center[2] in collaboration with IBM, which proposes to implement a comprehensive dashboard for the whole city in order to ensure resources optimisation and assist public authorities in preserving public order and safety.

But citizens are also being monitored by other types of sensors located not only throughout the territory, but also within their own hands. Increasingly, citizens are being tracked by communicating smart-devices: computers, tablets, smart-phones or other interactive devices which constantly collect data (including personal data) from their surrounding environment, aggregate them into a central database and process them with a view to better understand the current state of affairs, or even anticipate potential problems and risks.
Despite the significant costs it might entail in terms of privacy and data protection, such a massive collection and analysis of data can, however, hardly be avoided. Indeed, smart cities *need* to collect information about their citizens, in order to better understand their characteristics, behaviours, and needs, so as to provide them with a more customized service that is likely to increase the city's standard quality of life. More and more people are thus willing to give up their privacy, for the sake of obtaining a more customized or personalized service. They explicitly or implicitly accept to be physically tracked by their own smartphones, cameras, RFID chips, as well as to have their online activities monitored by cookies, beacons, or other tracking devices, so as to ultimately benefit from new and innovative services that rely on their own personal data in order to better satisfy their most inherent needs. This, of course, brings up the difficult question of where shall we draw the line between what constitutes a personalized service that is actually geared towards the interests of end-users, and what should instead be regarded more as a form of target advertising geared towards the interests of the advertisers. Most importantly, is such a distinction still useful, or are these formerly two distinct approaches actually merging into each other within this new integrated environment?

[1] The Domain Awareness Center (DAC) is a planned surveillance hub which aims to integrate public and private cameras and sensors all over the City of Oakland into one $10.9M mass surveillance system. For more information, see http://oaklandwiki.org/domain_awareness_center

[2] IBM Intelligent Operations Center for Smarter Cities provides an executive dashboard to help city leaders gain insight into all aspects of the city. For more details, see www.ibm.com/software/products/en/intelligent-operations-center

The problem is that - thus far - virtually every attempt at the deployment of smart cities has been undertaken by either corporate or governmental institutions. While the former are for the most part driven by economic incentives, the latter are torn between the desire to provide a service of public utility and the need to ensure public order and national security. And yet, in spite of their different motivations, both are likely to favor a model that promotes a regime of generalized surveillance, which is naturally likely to impinge upon the privacy of individual citizens.
In order to be successful in the long-run, any initiative aimed at providing new and innovative services to guide or support citizens in their daily interactions with the urban environment should give citizens a say on the manner in which, and the extent to which service providers are entitled to collect, use and reuse personal data. Most importantly, in order to remain in line with the provisions of the new European data protection regulation,[3] data collection and analysis should only be done with the explicit and informed consent of the data subject (Article 6) and citizens should be given the choice to opt in and out of these initiatives (Article 4) subject to full disclosure as regards the policies for information retrieval and procedures for information sharing (Article 15). Yet, most of smart cities which have been implemented so far fall short of some of these basic requirements (Allwinkle & Cruickshank, 2011).

Most of the problem inherent to privacy and data protection could be resolved if efforts towards smart cities deployment where not exclusively run by public authorities (driven by public polity and political goals) and private actors (whose interests are limited to short-term economic returns), but mostly by grassroots communities and civil society organisations, who actually have an incentive to promote the greater good (Townsend, 2013). Indeed, if the aim of smart cities is to improve citizens' QoL through greater efficiency and sustainability, the deployment of a smart city should not be dictated by any economic, corporate or governmental interest, but rather by the desire to further the interests of actual citizens. For this to be successful, there is a need for a more bottom-up and less corporate-led implementation of smart cities, relying on a grassroots, citizen-centric approach, combining integrated ICTs with active citizen participation and an intelligent management of physical, digital and informational resources (Caragliu & al. 2009). This is especially true in the context of communication infrastructures which represent one of the main vehicles for citizens to engage and participate in political, social and cultural life. While it is fundamental that municipalities provide the underlying technical infrastructure for telecommunications, and it is useful that private companies be allowed to compete to provide a more added-value service, today, citizens also need to realize the important role they might play in shaping the ground for grassroots innovation in the context of ICTs (Townsend, 2013).

3. Proposed solution: community mesh networks

In light of the growing interest (and need) for the deployment of modern ICTs and the lower infrastructure costs for wireless communications, decentralized approaches to networked communications are acquiring more and more momentum, both within civil society and elsewhere. Thus, in addition to top-down institutional projects aimed at the development of smart cities, citizens are progressively organizing into communities seeking to establish an interface for connecting the urban environment to the digital world, in ways which are more autonomous, self-sustainable and privacy-compliant than their commercial or municipal counterparts.
In this regard, community mesh networks (CMN) are an interesting example of grassroots decentralized communication infrastructures, whose architecture design has important implications on the deployment and configuration of smart cities, as well as on the way communities form and operate. A variety of initiatives have been developed thus far to support the deployment of decentralized mesh networks, allowing for a

[3] The European Commission plans to unify data protection within the European Union (EU) with a single law, the General Data Protection Regulation (GDPR). A proposal for a regulation was released on 25 January 2012. Subsequently numerous amendments have been proposed in the European Parliament and the Council of Ministers. The EU's European Council aims for adoption in late 2014 and the regulation is planned to take effect after a transition period of two years.

variety of devices, such as mobile phones, computers, and other wireless apparatuses to communicate directly to one another without passing through any centralized server or authority.
Ad-hoc mesh networks are decentralized network infrastructures that rely on a distributed and loosely coordinated network of peers contributing their own resources to the network so as to provide Internet connectivity to a specific community without relying on any pre-existing network infrastructure. They are also more robust than traditional centralized networks, in that they can dynamically adapt to changes in their surroundings and automatically reconfigure themselves according to the current availability of resources: if a new node appears, it will be automatically connected to the rest of the network, without the need for any additional configuration; if a node fails or disappears, the network will automatically reconfigure itself in order to route around it.
By means of a decentralized network infrastructure, mesh networks promote a more democratic, communitarian and participatory approach to network governance. As opposed to centralized network infrastructures which are generally owned and managed by third parties (be them either private or public institutions) CMN are operated *by* the community and *for* the community. They are autonomous citizen-centric communication infrastructures, designed to preserve the autonomy and the fundamental rights of individuals, by making every individual user responsible for the provision and redistribution of network connectivity, but also in charge of routing the traffic throughout the network.

a. Privacy and Security

Mesh networks could potentially provide a solution to the privacy concerns raised by centralized smart cities infrastructures, by promoting an open, decentralized, peer-to-peer approach to network infrastructure and connectivity.
Thus far, most CMN have been deployed as "open networks" promoting the principles of network neutrality and preserving individual rights, such as privacy and freedom of expression. Indeed, the decentralized character of mesh networks ensures that there is no single entity that controls the network: this means that there are no intermediaries or gatekeepers that might censor, filter, or perhaps even disclose information to corporate or governmental entities. As such, mesh networking represents a way to preserve the confidentiality of online communications. Given the lack of a central authority that regulates access to the network, it is extremely difficult for anyone to assess the real identity of users connected to these networks.
Besides, most of the open-source equipment that is used in the context of many mesh networks enables citizens to remain in control of their own data. To the extent that they have full control over their own devices, users' right to privacy is less likely to be infringed upon, as users are free to determine the manner in which and the extent to which their devices can collect personal data and communicate it to other connected devices. Citizens can assemble their own devices, deploy their own mesh networking kit, install their own software and manage their own data through it. They can even decide to share their personal data with their closest friends or, more broadly, to a larger community, but only according to the conditions that they have individually chosen.
In the context of smart cities, this mean that citizens can enjoy the benefits of more customized and personalized services, which are tuned to and automatically adapt to evolving users' needs, without having to renounce to their privacy nor let go of their right to data protection.

Greater privacy does not, however, necessarily lead to greater security. While citizens can more effectively control the collection and/or use of their personal data, it remains nonetheless important to ensure that such data actually remains safe from unauthorized access by third parties. As every device connected to an open network is potentially insecure, malicious users could try and hack into the system in order to get hold of sensitive data, alter the device's functionalities, or even just corrupt the system by introducing a virus or malware. Besides, even if they not are not (directly) connected to the global Internet network, it is, of course, still possible for malicious third parties - which are locally connected to a domestic mesh network - to monitor the traffic transiting through that network. The technology cannot, by itself, be used to conceal one's identity, nor to provide strong security over the network traffic. It is, in fact, the "open" design of many community mesh networks that makes them inherently insecure: if anyone is entitled to join the network either as a client or a relay node transferring packets throughout the network, then anyone locally connected to that network is also capable of intercepting (or sniffing) these packets. Unless users employ end-to-end encryption, the content of all messages and communication can be easily monitored by third parties. In fact,

even with encryption, it is still possible to collect metadata (i.e. who sent what to whom) unless one uses an overlay network, such as Tor or Cjdns, to obfuscate the source and/or destination of communications.[4]
In this sense, mesh networks do not provide any more protection against surveillance by either governmental or corporate entities than the global Internet does. They do, however, contribute to changing the rules of the games and the corresponding power dynamics, by making users more autonomous, informed and aware, and by giving them the ability to control the extent to which data is being collected and the manner in which such data is being transmitted through the network. Indeed, to the extent that the network is not deployed by any third party, it is for the community itself to ultimately decide the manner in which the network should effectively be designed and implemented.

b. Citizen-centric technologies

What is really revolutionary about mesh networking is not the novel use of technology, but rather the fact that it provides a means for people to organise into communities and share resources amongst themselves. Although originally designed to overcome situations of crisis (Portmann & Pirzada, 2008) or to escape from the oppressive control of totalitarian regimes (Hasan & al., 2013), mesh networks have thus far been deployed by several communities and civil society organisations as a means to experiment with new models of governance: an inclusive form of governance based on participation and collaboration among peers.
By analogy with the concept of commons-based peer production (Benkler, 2006), CMNs constitute an attempt at transposing the concept of open source cooperation in the physical world. By virtue of their decentralized character, these networks requires a communitarian and participatory approach to Internet communication.The creation of a mesh network is ultimately collective process, which requires the participation of every member of the community to produce a common platform of communication, whose utility is generally greater than the sum of its parts. Individual users contribute with their own resources to the overall operations of the network -- and the greater is the number of users, the greater becomes the value of the network as a whole.
Indeed, given that CMNs are generally deployed to satisfy the needs of a particular community, community members have an incentive to provide resources to the network, so as to maximize the benefits they can derive from it, both individually and collectively. Although each individual user of the network might have personal (and sometimes conflicting) interests, all have an interest in contributing to the network insofar as they can reap the benefits from it. This is exactly the kind of spontaneous collaboration that feeds into the systems and encourages the public to provide more and more resources to distributed peer-to-peer networks (see e.g. Golle & al., 2001; Ranganathan & al., 2003; Antoniadis & al., 2004).

An interesting application of CMN with reference to smart cities is illustrated by the Smart Citizen project, an initiative launched by Tomas Diez (director of Fab Lab Barcelona) aimed at empowering citizens to achieve a better quality of life by supporting and promoting more citizen's participation in better understanding and improving the city they live in. The Smart Citizen kit is an Arduino-operated device that comes with a set of low-cost modular open hardware sensors that can be used to capture, process and analyse real-time environmental data (such as air quality, temperature, sound or humidity). By creating a mesh network of such sensors, data collected by a variety of citizens can be shared on the Smart Citizen platform to be subsequently aggregated into a common database from which new knowledge or indicators can be extracted. The goal is, ultimately, to allow for citizens to collaborate together towards the construction of a more sustainable environment through a more efficient urban development.
Citizens can thus play a key role in the design of smart cities by providing the means to assess the effectivity of urban policies geared towards improving community, civic and social life in the city. Yet, as opposed to the traditional approach to smart city deployment (where a large number of sensors are installed throughout the city to collect data about citizens without them even being aware of it), with the Smart Citizen project, those are the individuals themselves who are collecting data about their own environment, by relying only and exclusively on their own devices. In this sense, citizens are no longer regarded as mere data-subjects, but rather assume a more active role as data-providers. They contribute - either implicitly or explicitly - to the

[4] TOR (The Onion Router) and CJDNS are two publicly accessible overlay networks that provide anonymity to their users by encrypting and routing their requests through a number of peer nodes to disguise the real origin of the traffic.

urban environments by interacting with specific applications which have been deployed to collect data directly from the individuals who are the most concerned with a particular issue, and the most eager to benefit from a service that is more suited to the needs of their particular community. Data might either refer to the urban environment (see e.g. Fillthathole.org.uk, where citizens can report holes in the roads, for the city to fix them; WideNoise, an application that uses the IPhone microphone to measure the decibels at a specific location) or to the individual themselves (see e.g. Asthmapolis developed a tool for asthma patients, allowing them to monitor and publicly disclose their medical activities, in the hope that public health agencies will eventually make use of the data collected to improve their health). Because they are actually in control of their own devices, and given that they know exactly what kind of data they are sharing with whom, individuals are likely to be more *willingly* to share information (even personal information) with each other -- if they believe they can either individually benefit from it, or, to the least, contribute to the greater good. Most importantly, because they are not dependent on any third party, citizens are better equipped to satisfy their own needs by their own means, without having to compromise between privacy and utility. With mesh networking, community members can reclaim control over their own means of communication, and consequently decide, by themselves, what are the underlying functionalities and technical features they want to implement. Ideally, this would lead to the deployment of smart cities run by *smart citizens*, driven by the desire to build new and innovative structures capable of providing highly customized and personalized services which promote democratic values and preserve civil liberties and fundamental rights.

Future research directions

Of course, there are currently only a minority of people capable of deploying a mesh network. Most mesh networks were initiated by a few tech savvy communities with a strong commitment to openness, inclusiveness and transparency (De Filippi & Tréguer, 2014). Today, however, most users are passively using the network and do not understand the underlying complexity that is required to manage these networks. Yet, as Wikipedia has shown, the power of the digital era is that the work of a few can actually affect the reality of many (Kittur & al., 2007). All the system need is a small number of experts capable of setting up the basic infrastructure in such a way that others can subsequently benefit from it - and, ideally, contribute their own resources to the system.
Mesh networks were initially difficult to deploy. Since every node acts both as a client and as a relay node, users need to set up their own server and configure it to use the appropriate routing protocol before they can use the network. Configuration is challenging to the inexperienced users, and can be very time-consuming even for the most experienced ones.

Today, the situation has changed drastically. A few years ago, the Commotion Wireless[5] project (an initiative from the Open Technology Institute of the New America Foundation) began working on the "Internet in a suitcase" project: an Open Source toolkit that can be readily installed on a variety of low-cost, off-the-shelf devices for anyone to set up a mesh network without any technical knowledge. The project, which was originally motivated by the need to provide a secure and reliable platform to prevent authoritarian governments from controlling or blocking dissident or activist communications (King, 2011) has now become one of the most popular tools for mesh network deployment around the globe (for more details, see *http://www.commotionwireless.net*). Similar tools are also being developed by other communities - such as MeshNet (*https://projectmeshnet.org*), NodeWatcher (*http://dev.wlan-si.net/wiki/Nodewatcher)*, or the Serval Project in Australia (*http://www.servalproject.org*) - whose goal is, ultimately, to allow anyone to deploy the necessary software infrastructure to enable direct communications between a variety of user's devices. Some communities even went one step further, by providing pre-installed and pre-configured hardware devices - such as the Open-Mesh routers from MIT that only need to be plugged into an electrical outlet (and, ideally, to an Internet connection) to provide connectivity on-the-fly (see *http://open-mesh.com* for more details).
But mesh networking technologies are also progressively being deployed on our everyday's devices. Just a few months ago, Open Garden released FireChat (*https://opengarden.com/firechat*), a proprietary end-user

[5] Commotion Wireless is an open-source wireless mesh network for electronic communication. The project was developed by the Open Technology Institute, and development included a $2 million grant from the United States Department of State in 2011 for use as a mobile ad hoc network (MANET). For more details, see https://commotionwireless.net/

application making use of Apple's new bluetooth multi-peer mesh networking capabilities provided by iOS 7 to enable anyone with an iPhone or an Ipad to set up a modular ad-hoc mesh network. It only took a few weeks for a similar functionality to be enabled on Android phones, so that both iOS and Android users can now communicate on the same mesh network. As more and more of such applications get deployed into standard end-user devices, we might soon witness the emergence of a more grassroots and citizen-centric approach to smart cities, with the deployment of an IoT that ultimately relies on grassroots applications of mesh networking technologies.

The flip-side is, however, that grassroots community networks can only subsist insofar as there is someone willing to contribute to the network. As opposed to software, which, once produced, remains operational and available to all (even if the community no longers assign any resources to further develop it), WCNs cannot operate without a constant provision of resources to sustain the infrastructure. In order to ensure the long-term sustainability of the network and maximize the benefits that they can derive from the network (both individually and collectively), users need to provide resources to the system and work together to resolve any network failure that might occur over time (as a result, e.g. of a router breakdown or a displaced radio antenna). Although mesh networks might allow for the establishment of supernodes (which have priority over the other nodes by virtue of their greater bandwidth, for instance), all users eventually contribute to increasing the overall network bandwidth. This is especially true in the context of ad-hoc mesh networks based on dynamic routing protocols where the efficiency of the network ultimately depends on the number of users who accept, at any given moment, to operate as relay nodes.

One important question in this regard relates to the incentive mechanisms that could be employed to encourage citizens to contribute with their own resources to the deployment of grassroots smart city environments. Beyond the ideological values related to privacy and autonomy, additional benefits must be extracted for such an alternative approach to enter into the mainstream.

A number of WMN are currently experimenting with innovative mechanisms to incentivize participation and to encourage users contributions to the network. A particularly interesting solution is CommunityCoin, an initiative proposed by the Guifi[6] community network. CommunityCoin is a crypto-currency based on the same technology as Bitcoin, which has been specifically designed for network communities. It features a mechanism of rewards based on the contribution and participation of community members to the overall operation of the network. This currency can, however, only be used for the internal community workaround: users contributing their resources to the network will be able to spend the CommunityCoins they receive in order to e.g. buy a second hand hardware from another community member. The goal is, ultimately, to incentivate the members to work for the community (installing new nodes, creating new services, etc.) and make the community network self-sustainable.

Of course, mesh networking only represents one small (albeit critical) part of the overall smart city infrastructure. Technology can (and should) also be deployed to elaborate and deploy innovative systems of governance, encouraging citizens to be much more responsible, and perhaps more responsive to their own needs. A truly emancipatory technology should not only provide the means for citizens to become more independent and autonomous within their own city, but also to exercise greater control and oversight over the municipality. A potential solution to the latter is the MuniBit initiative, launched by Zachary Caceres from the Startup Cities Institute,[7] which proposes to rely on distributed cryptoledgers (the underlying technology of Bitcoin) to improve transparency of government finances in the developing world, by inviting citizens to actively participate in the verification and execution of all financial transactions stemming from local authorities (in order to preclude fraud or corruption), as well as to eventually become shareholders in their local government, and contribute to political decisions through a transparent digital process (Swanson, 2014). Here, again, the technology incorporates the political goal of encouraging the establishment of strong

[6] Guifi.net is a free, open telecommunications community network, which is self-organized: all nodes of the network are contributed by individuals, companies or institutions that provide their own resources to provide the infrastructure and content that might not otherwise be accessible.

[7] Startup Cities Institute (SCI) is a non-profit research organization that studies the use of startup communities for legal and political reform. Startup Cities are small and highly autonomous jurisdictions established within pre-existing nations. They can be used to create inclusive economic growth, combat corruption and insecurity, and to test public policy innovations in public services, transparency, and environmental stewardship. SCI is a project of Universidad Francisco Marroquín in Guatemala City.

and cohesive communities capable of self-organizing in order to fulfill their own needs, by their own means.

Conclusion

The deployment of smart cities and the IoT are providing considerable advantages to many citizens eager to experience new social connections and interactions within the urban environment. Yet, by reason of their centralized character and the extensive degree of data collection they entail, the current approach to smart-city deployment is often highly intrusive and might substantially hinder the citizens' right to privacy and data protection.

Are citizens thus expected to trade-off their privacy for the sake of greater comfort or efficiency? Quite the contrary. The need to align innovation policies for smart cities deployment with better urban development and greater citizen empowerment requires reconsidering the role of citizens as the central focus of smart cities development. Indeed, beyond the initial deployment of smart devices, the development and long-term sustainability of smart cities requires the development of innovative technologies and infrastructures capable of promoting participation and social inclusion in the cities of tomorrow. Yet, in order to do so, the general approach to smart cities deployment must integrate the social component to the technical component.

Through the deployment of mesh networks, citizens can set up their own smart-city environments, by connecting several devices together in a decentralized fashion within a peer-to-peer network. These devices can interact with a multitude of devices connected to one another, so as to coordinate themselves, without the need for a centralized authority.

Ideally, this would lead to the establishment of an open and decentralized network infrastructure (composed of a variety of citizen-owned sensors or devices) which is empowering citizens with innovative interactive and customized services, so as to increase their overall quality of life, while remaining in compliance with the fundamental rights of privacy and data protection. Indeed, to the extent that citizens are in charge of setting up and managing the networks, those are likely to be deployed in such a way as to better respect the privacy and autonomy of users -- who can benefit from the same advantages and functionalities provided by traditional smart cities environments, without the costs of centralized control.

Accordingly, by relying on community mesh networks, as opposed to third party infrastructures, cities can be "smart" while also respecting the intelligence of their citizens. Paradigmatically, the creation of independent network infrastructures regulated through innovative model of governance become a key prerequisite for the involvements and participation of smart citizens to smart cities deployment.

References:

Allwinkle, S., & Cruickshank, P. (2011). Creating smart-er cities: An overview.*Journal of Urban Technology*, *18*(2), 1-16.

Antoniadis, P., Courcoubetis, C., & Mason, R. (2004). Comparing economic incentives in peer-to-peer networks. *Computer networks*, *46*(1), 133-146.

Bauman Z. and Lyon D. Liquid Surveillance: A Conversation. Polity Press, Cambridge – Malden. 2013.

Bauwens, M. (2005). The political economy of peer production. CTheory, 1.

Bazzanella L., Roccasalva G. and Valenti S., Phigital Public Space Approach: A Case Study in Volpiano, LAQ-Tip, DAD Politecnico di Torino, http://www.mifav.uniroma2.it/inevent/events/pcst_sce_2013/docs/I_5.pdf. 2013.

Benkler Y. The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press, New Haven – London. 2006.

Benkler, Y., & Nissenbaum, H. (2006). Commons□based Peer Production and Virtue*. Journal of Political Philosophy, 14(4), 394-419.

Brooks D., The Philosophy of Data, N.Y. Times, http://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html?_r=0. 2013

Caragliu, A., Del Bo, C. and Nijkamp, P. Smart cities in Europe. Serie Research Memoranda 0048. VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics. 2009.

De Filippi, P., Tréguer, F. (2014). Expanding the Internet Commons : The Subversive Potential of Wireless Community Networks, in Journal of Peer Production (forthcoming)

Golle, P., Leyton-Brown, K., Mironov, I., & Lillibridge, M. (2001). Incentives for sharing in peer-to-peer

networks. In *Electronic Commerce* (pp. 75-87). Springer Berlin Heidelberg.
Hasan, S., Ben-David, Y., Fanti, G., Brewer, E., & Shenker, S. (2013). Building Dissent Networks: Towards Effective Countermeasures against Large-Scale Communications Blackouts. In *Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet, FOCI* (Vol. 13).
Healy, K., & Schussman, A. (2003). The ecology of open-source software development. Unpublished manuscript, January, 29, 2003.
Humphries, C. (2013). The too-smart city. The Boston Globe, 19.
King R. (2011). "Building a Subversive Grassroots Network". *Spectrum*. Institute of Electrical and Electronics Engineers.
Kittur, A., Chi, E., Pendleton, B. A., Suh, B., & Mytkowicz, T. (2007). Power of the few vs. wisdom of the crowd: Wikipedia and the rise of the bourgeoisie.*World wide web*, *1*(2), 19.
Lessig, L. (2004). Free culture: How big media uses technology and the law to lock down culture and control creativity. Penguin.
Madden, M. (2007). *Digital Footprints: Online identity management and search in the age of transparency*. Washington, DC: Pew Internet & American Life Project.
Martinez-Balleste, A., Perez-Martinez, P.A. and Solanas, A., The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City is Possible. IEEE Communications Magazine, Vol. 51. 2013.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.Consulted, 1, 2012.
Nam T. and Pardo T.A, Smart City as Urban Innovation: Focusing on Management, Policy, and Context. Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance. 2011.
O'Mahony, S., & Ferraro, F. (2007). The emergence of governance in an open source community. Academy of Management Journal, 50(5), 1079-1106.
Portmann, M., & Pirzada, A. A. (2008). Wireless mesh networks for public safety and crisis management applications. *Internet Computing, IEEE*, *12*(1), 18-25.
Raymond, E. (1999). The cathedral and the bazaar. Knowledge, Technology & Policy, 12(3), 23-49.
Steventon, A. and Wright, S. (eds), Intelligent Spaces: The Application of Pervasive ICT. Design at Work: Cooperative Design of Computer Systems. Springer-Verlag, London. 2006.
Ranganathan, K., Ripeanu, M., Sarin, A., & Foster, I. (2003). To share or not to share: An analysis of incentives to contribute in collaborative file sharing environments. In *In Workshop on Economics of Peer-to-Peer Systems*.
Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. Journal of Sensor and Actuator Networks, 1(3), 217-253.
Swanson, T. (2014). Great chain of numbers: a Guide to Smart Contracts, Smart Property and Trustless Asset Management. Amazon Digital Services, Inc.
Townsend, A. M. (2013). *Smart cities: big data, civic hackers, and the quest for a new utopia*. WW Norton & Company.
Want, R., & Pering, T. (2005, May). System challenges for ubiquitous & pervasive computing. In Proceedings of the 27th international conference on Software engineering (pp. 9-14). ACM.